Joint ESAs public event on DORA, technical discussion

6 February 2023

EBA EUROPEAN BANKING AUTHORITY

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

SESSION 1:

RTS on ICT risk management framework
RTS on simplified ICT RMF
RTS to specify the policy on ICT services
RTS to specify elements when sub-contracting critical or important functions

Barbara Daskala, Senior Supervision Officer ESMA

ICT Risk Management and ICT third party risk

Objectives and general overview

The aim is for a comprehensive, strong and effective ICT risk management

- Tackle fragmentation of ICT requirements laid down in the current Union financial services law
- Upgrade ICT risk requirements
- Achieve consistency in rules
- Promote risk-based implementation and supervision
- Covering explicitly cyber hygiene
- Introduce key principles for financial entities' management of ICT third-party risk
- Complement existing requirements on ICT outsourcing
- Enable monitoring of the ICT third party contractual arrangement (not anchored fully into Union law before DORA)
- Achieve homogeneity and convergence on the monitoring of ICT third-party risk and ICT third-party dependencies
- Considering size, the overall risk profile of the financial entity, the nature, scale and complexity of its services, activities and operations.

RTSs on ICT Risk Management – Legal Mandate

JC in consultation with ENISA

Article 15 Further harmonisation of ICT risk management tools, methods, processes and policies	Article 16 Simplified ICT risk management framework*
a. Specify **further elements to be included in the ICT security policies, procedures, protocols and tools** (Article 9(2)) b. Develop further **controls of access management rights** and **monitoring of anomalous behaviour** (Article 9(4), point (c)) c. Develop further mechanisms on **prompt detection of anomalous behaviour** related to ICT risk (Article 10(1)) and **triggering of incident detection and response processes** (Article 10(2)) d. Specify further **ICT business continuity policy components** (Article 11(1)) e. Specify further **ICT business continuity plan testing** (Article 11(6)) f. Specify further **ICT response and recovery plans** components (Article 11(3)) g. Specify further **content and format of the report on the review for the ICT RM framework** (Article 6(5))	a. Specify **further elements to be included in the ICT risk management** (Article 16(1)(a)) b. Specify **further elements in relation to systems, protocols and tools** to minimise the impact of ICT risk (Article 16(1)(c)) c. Specify **further components of the ICT business continuity plans** (Article 16(1)(f)) d. Specify **further rules on business continuity plan testing** (Article 16(1)(g)) e. Specify **further content and format of the report on the review for the ICT RM framework** (Article 16(2)) ***For small and non-interconnected investment firms, payment institutions exempted; institutions exempted; electronic money institutions exempted; and small institutions for occupational retirement provision (Article 16(1), first subparagraph)**

RTSs on Third Party Risk Management – Legal Mandate

Article 28(10) To further specify the content of the policy on the use of ICT services concerning critical or important functions provided by ICT third-party service providers	Article 30(5) To specify elements when sub-contracting services supporting critical or important functions
Under Article 28 (2) of DORA, as part of their ICT risk management framework, financial entities, other than financial entities referred to in Article 16(1) and other than microenterprises, shall adopt, and regularly review, **a strategy on ICT third-party risk**, taking into account the multi-vendor strategy referred to in Article 5(9) where applicable. **The strategy on ICT third-party risk shall include a policy** on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and shall apply on an individual and, where relevant, on a sub-consolidated and consolidated basis. […]	In accordance with Article 30(2) (a) of DORA, the contractual arrangements on the use of ICT services shall include at least the following: (a) a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, **indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when this is the case, the conditions applying to such subcontracting.**
In accordance with Article 28 (10) of DORA, the ESAs shall, through the Joint Committee, develop **draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2** in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. When developing those draft regulatory technical standards, the ESAs shall take into account the size, nature, scale, complexity and overall risk profile of the financial entities.	Article 30 (5) of DORA sets out that the ESAs shall, through the Joint Committee, develop **draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.**
Deadline: 12 Months	**Deadline:** 18 Months

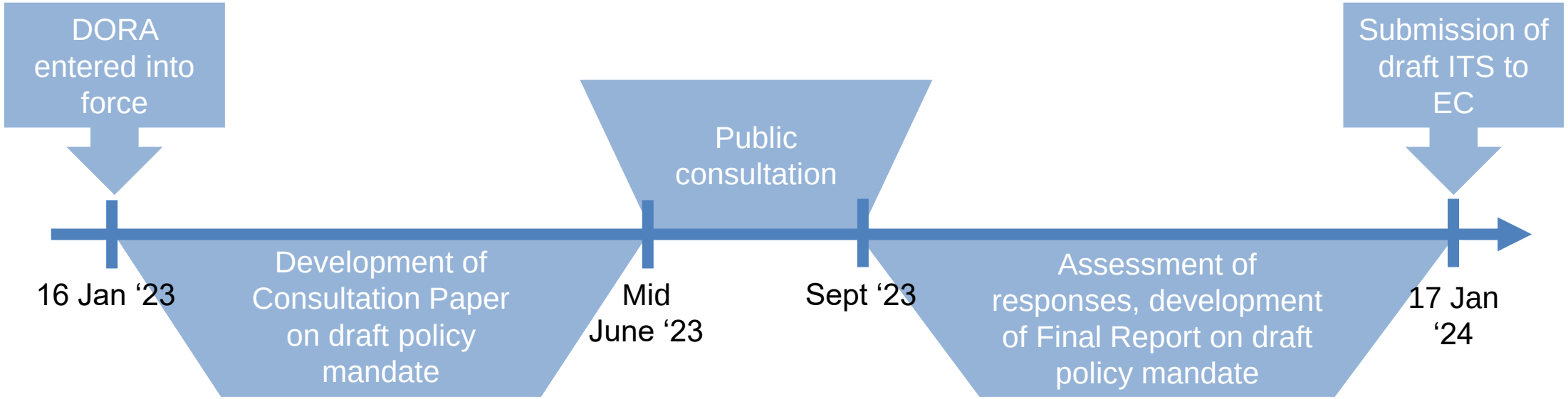
EBA EUROPEAN BANKING AUTHORITY

eiopa European Insurance and Occupational Pensions Authority

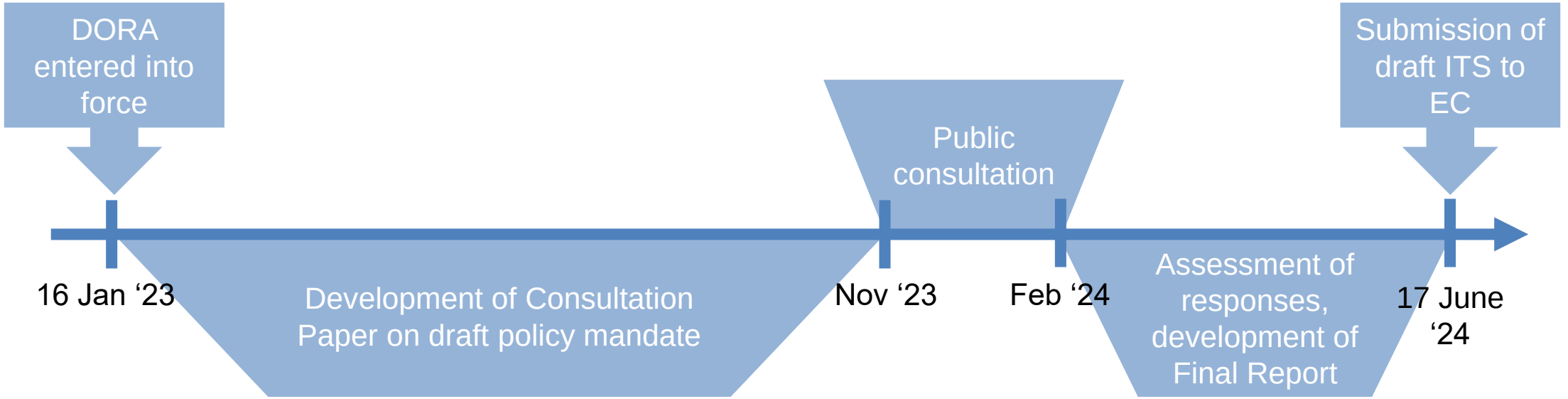
ESMA European Securities and Markets Authority

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Preliminary Timeline for RTSs on RMF and ICT Policy (12 months deadline)



Preliminary timeline RTS on sub-contracting (18 months deadline)



SESSION 2:

RTS on classification of major ICT incidents
RTS on reporting of major ICT incidents

Antonio Barzachki, Senior Expert EBA

Overview of DORA's major ICT-related incident reporting (1)

DORA introduces harmonised and streamlined framework for reporting of major ICT-relates incidents where financial entities:

- establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.
- report major ICT-related incidents to the relevant competent authority under DORA by way of initial notification, intermediate report and final report.
- report, on voluntary basis, significant cyber threats to the relevant competent authority under DORA.

Recipients of the major ICT-related incident reports (based on respective competences)

- Relevant competent authorities
- EBA, ESMA or EIOPA
- ECB
- competent authorities, single points of contact or CSIRTs under NIS2
- resolution authorities
- other public authorities.

Notification of relevant competent authorities in other Member States - based on assessment by the EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and the relevant home competent authorities.

Overview of DORA's major ICT-related incident reporting (2)

Criteria for classification of major ICT-related incidents:

a) the number and/or relevance of **clients or financial counterparts affected** and, where applicable, the amount or number of **transactions affected** by the ICT-related incident, and whether the ICT-related incident has caused **reputational impact**;

b) the **duration** of the ICT-related incident, including the service downtime;

c) the **geographical spread** with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;

d) the **data losses** that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;

e) the **criticality of the services affected**, including the financial entity's transactions and operations;

f) the **economic impact**, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.

Classification of cyber threats as significant

Based on the **criticality of the services at risk**, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.

Overview of the legal mandate on the RTS on classification of major ICT incidents

Article 18(3) and (4)
RTS on criteria for classification of major ICT-related incidents and significant cyber threats

The ESAs shall, through the Joint Committee, and in consultation with the ECB and ENISA, develop draft RTS to further specify the following:

a) *the **criteria** set out in paragraph 1, including **materiality thresholds for determining major ICT-related incidents** or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1);*

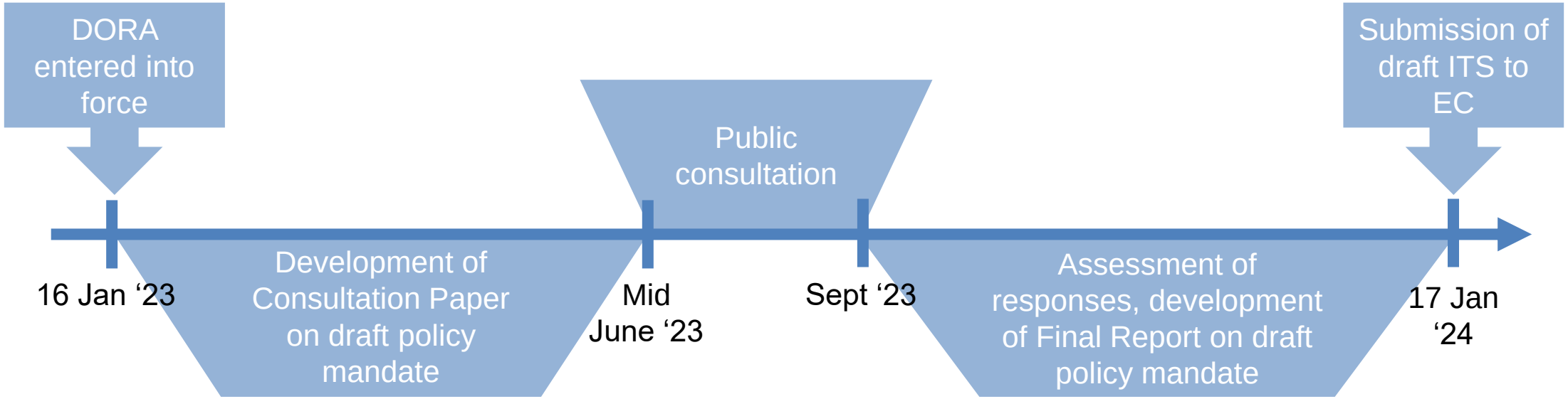
b) *the **criteria** to be applied by competent authorities for the purpose of **assessing the relevance** of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, **to relevant competent authorities in other Member States**', and the **details of reports** of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, **to be shared with other competent authorities** pursuant to Article 19(6) and (7)*

c) *the criteria set out in paragraph 2 of this Article, including high materiality thresholds for determining significant cyber threats.*

*When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2) **[proportionality principle]**, as well as **international standards, guidance and specifications developed and published by ENISA**, including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly.*

Deadline: 12 Months

Preliminary Timeline for the RTS on classification of major ICT incidents (12 months deadline)



Overview of the legal mandate on the RTS on reporting of major ICT incidents

Article 20(a)
RTS specifying the content of the major ICT-related incident reports and notifications for significant cyber threats, as well as the time limits for incident reporting

The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop common draft regulatory technical standards in order to:

i. *establish the **content of the reports for major ICT-related incidents** in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not;*

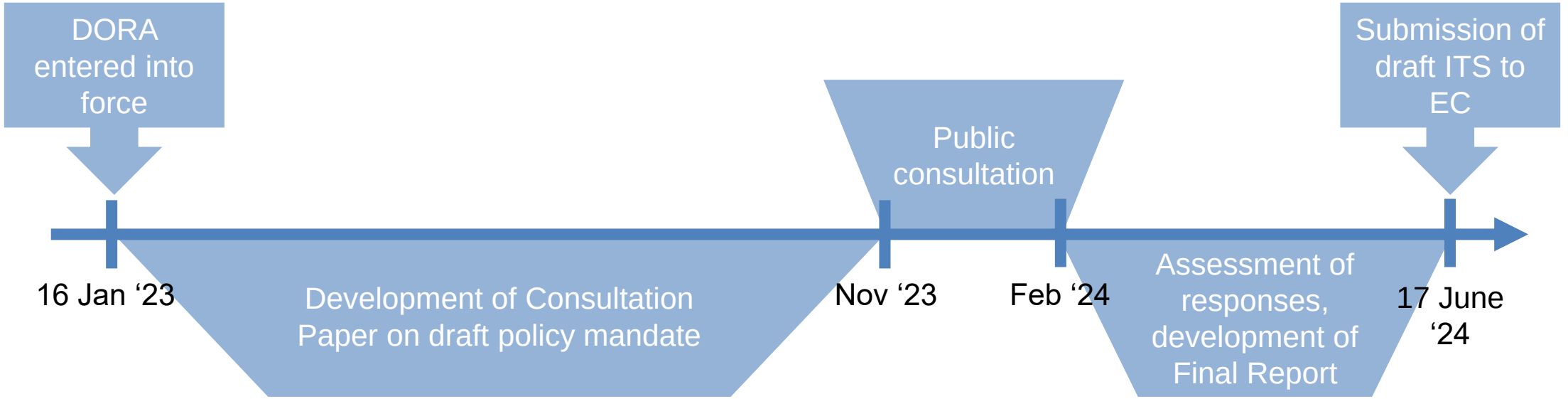
ii. *determine the **time limits for the initial notification and for each report** referred to in Article 19(4);*

iii. *establish the **content of the notification for significant cyber threats**.*

*When developing those draft regulatory technical standards, the ESAs shall take into account the **size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations**, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), **different time limits may reflect, as appropriate, specificities of financial sectors**, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555. The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of that Directive;*

Deadline: 18 Months

Preliminary timeline for the RTS on reporting of major ICT incidents (18 months deadline)



SESSION 3: ITS on register of information

Andrea Vetrone, Senior Expert EIOPA

Overview of the legal mandate

Article 28(9) ITS on Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third–party service providers

The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the ***register*** *of* ***information*** *referred to in paragraph 3****, including information that is common to all contractual arrangements on the use of ICT services****.*

Article 28 (3) Register of Information

As part of their ***ICT risk management framework****, financial entities shall* ***maintain and update*** *at* ***entity level*** *and, at* ***sub-consolidated*** *and* ***consolidated levels****, a* ***Register of Information*** *in relation to* ***all contractual arrangements on the use of ICT services provided by ICT third-party service providers.***

The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not.

Financial entities shall report at least yearly to the competent authorities information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided.

Financial entities shall make available to the competent authority, upon its request, the full Register of Information or as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity.

Financial entities shall inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services concerning critical or important functions and when a function has become critical or important.

EBA EUROPEAN BANKING AUTHORITY

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

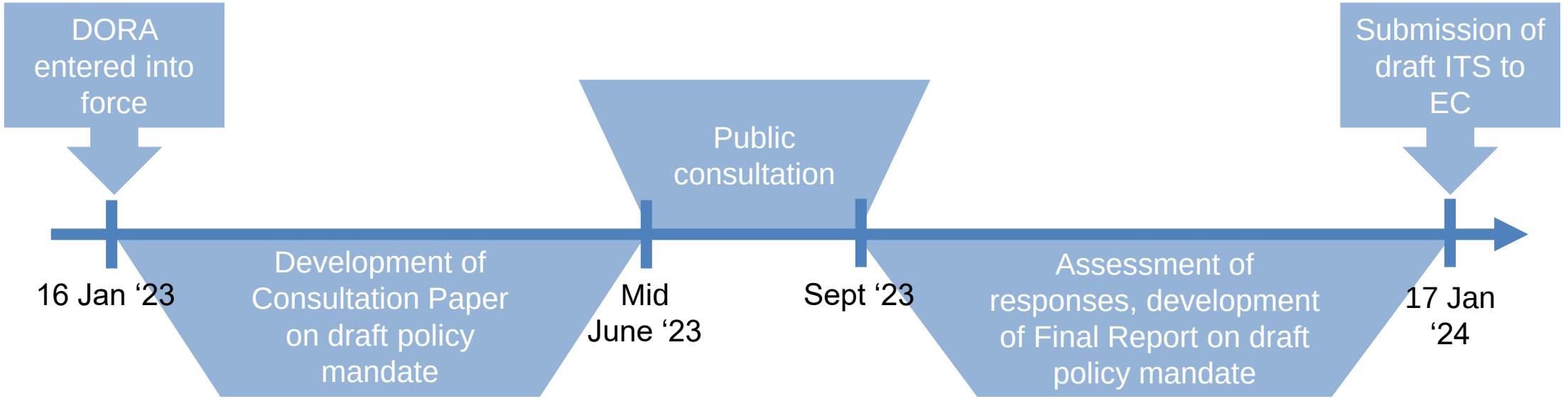
JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Deadline: 12 Months

Purpose of the register of information

Financial entities ICT risk management	***As part of their ICT risk management framework, financial entities shall maintain and update*** *at entity level and, at sub-consolidated and consolidated levels,* ***a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers****. (Art 28.3)*
Supervision by competent authorities	***Financial entities shall make available to the competent authority****, upon its request,* ***the full Register of Information*** *[…] along with any information deemed necessary* ***to enable the effective supervision of the financial entity*** *(Art. 28.3)*
Designation of critical third-party providers	*To enhance supervisory awareness of ICT third-party dependencies, and* ***with a view to further supporting the work in the context of the Oversight Framework*** *established by this Regulation, all financial entities should be required to maintain a register of information with all contractual arrangements about the use of ICT services provided by ICT third-party service providers. (Recital 65)*

Preliminary Timeline for the ITS on the register of information (12 months deadline)



SESSION 4: Call for advice on criticality criteria

Andrea Vetrone, Senior Expert EIOPA

Legal Background

- DORA Regulation introduces a Union Oversight Framework for ICT third-party providers (ICT TPPs) deemed critical (CTPPs)
- ESAs to monitor activity of CTPPs on a pan-European scale
- ESAs to designate CTPPs for this monitoring exercise (Article 31(1))
- Article 31(2) sets out 4 high-level criteria to assess criticality of ICT TPPs
- Criticality criteria should also be applied in case of voluntary opt-in by an ICT TPP (Article 31(11))

Article 31(6): Empowers the Commission to adopt a delegated act to further specify criticality criteria by July 2024

- *Note: the call for advice also covers the determination of the amount of the oversight fees and the way in which they are to be paid by CTPPs. This topic is not covered during this event.*

High-Level Criticality Criteria: Article 31(2) DORA Regulation

High-level Criterion 1	The **systemic impact on the stability, continuity or quality of the provision of financial services** in the event that a CTPP would face a large-scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the CTPP provides services.
High-level Criterion 2	The **systemic character or importance of the financial entities that rely on a CTPP**, by taking into account: i. the number of global systemically important institutions (**G–SIIs**) or other systemically important institutions (**O–SIIs**) that rely on the CTPP, and ii. the **interdependence between the G–SIIs or O–SIIs** and other financial entities, including situations where the G–SIIs or O–SIIs provide financial infrastructure services to other financial entities.

High-Level Criticality Criteria: Article 31(2) DORA Regulation

High-level Criterion 3	The **reliance of financial entities on the services provided by a CTPP**, in relation to **critical or important functions** of financial entities that ultimately involve the same ICT TPP, irrespective of whether financial entities rely on those services directly or indirectly, through subcontracting arrangements.
High-level Criterion 4	The **degree of substitutability of a CTPP**, by taking into account: i. the lack of real alternatives, even partial, and ii. difficulties in relation to partially or fully migrating the relevant data and workloads from the CTPP to another ICT TPP.

Scope of the Call for Advice to ESAs

The Joint ESAs response should include:

- Several **specific sets of indicators** of both qualitative and quantitative nature per each of the 4 high-level criticality criteria set out in Article 31(2);
- Where applicable, **minimum thresholds** per indicator;
- **Background information** deemed relevant to support the build-up of indicators;
- If needed, **information necessary for Commission to correctly interpret indicators**;
- Provision of a **cost-benefit analysis** of all indicators considered;
- **Reflections on the frequency of reviewing criticality criteria**; and
- **Feedback statement** on public consultation.

Preliminary Timeline for the call for advice