Joint ESAs public hearing on the second batch of DORA policy products

23 January 2024

European Banking Authority

European Insurance and Occupational Pensions Authority

European Securities and Markets Authority

Programme

- **09:01-09:10 Opening**
- **09:10-09:20 Welcoming remarks**

  Verena Ross (Chairperson, ESMA)
- **09:20-09:30 Keynote speech**

  Gerry Cross (Chairperson, Joint Committee Sub-Committee on Digital Operational Resilience)
- **09:30-10:30 SESSION 1: RTS on oversight harmonisation**

  Andrea Vetrone (Senior expert, EIOPA) and Andra Remeur (Expert, EIOPA)
- **10:30-11:30 SESSION 2: : Guidelines on oversight cooperation and information exchange between ESAs-CAs**

  Andrea Vetrone (Senior expert, EIOPA)
- **11:30-11:45 Coffee break**
- **11:45-13:00 SESSION 3: RTS and ITS on major incident reporting**

  Antonio Barzachki (Senior policy expert, EBA)
- **13:00-14:00 Lunch break**
- **14:00-14:45 SESSION 4: Guidelines on cost and losses caused by major ICT-related incidents**

  Christoph Erkunt (Expert, EBA)
- **14:45-15:45 SESSION 5: RTS on subcontracting ICT services**

  Djamel Bouzemarene (Senior policy expert, EBA)
- **15:45-16:00 Coffee break**
- **16:00-17:00 SESSION 6: RTS on threat-led penetration testing**

  Karole-Anne Sauvet-Frot (Senior policy officer, ESMA)
- **17:00 End of the public hearing**

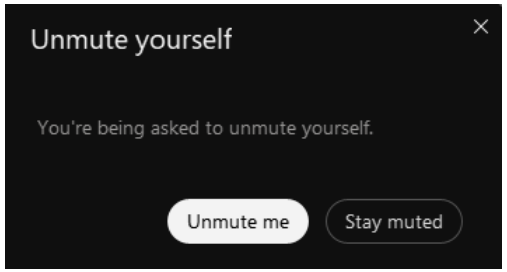
How to interact with us today: Slido

1. **Go to slido.com, enter event code #DORA and your full name and organisation (e.g. *"Mario Rossi (EIOPA)"*).**
   - The name and organisation used for Slido and WebEx must be identical.
2. **Submit written comments/questions through Slido and upvote questions of interest submitted by other participants.**
3. **If your question is very popular, we will read it during the meeting and may ask you to raise your hand via WebEx and orally explain it.**
   - The moderator will not accept inputs which are:
     - Submitted by people with uncompleted names
     - Offensive
   - Inputs related to areas of DORA not covered during this event, will be given a lower priority compared to those in scope
   - We will try to archive all inputs before each session.

How to interact with us today: WebEx

1. **If your input on Slido is selected and the moderator calls your name, you will have to raise up your hand in WebEx by using the "✋" button**

2. **Once the moderator gives you the word, you will receive a prompt on your screen to unmute yourself.**



- Please keep your intervention to max. 2 minutes to also allow others to share their views. Always indicate your name and organisation.
- Given time constraints, we kindly ask your understanding that not all participants may get the possibility to make an oral intervention.
- Don't raise up your hand unless your name is called. It doesn't worth it!

Welcoming remarks

Verena Ross, Chairperson of ESMA

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Keynote speech

Gerry Cross, Chairperson of the Joint Committee sub-committee on Digital Operational Resilience

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

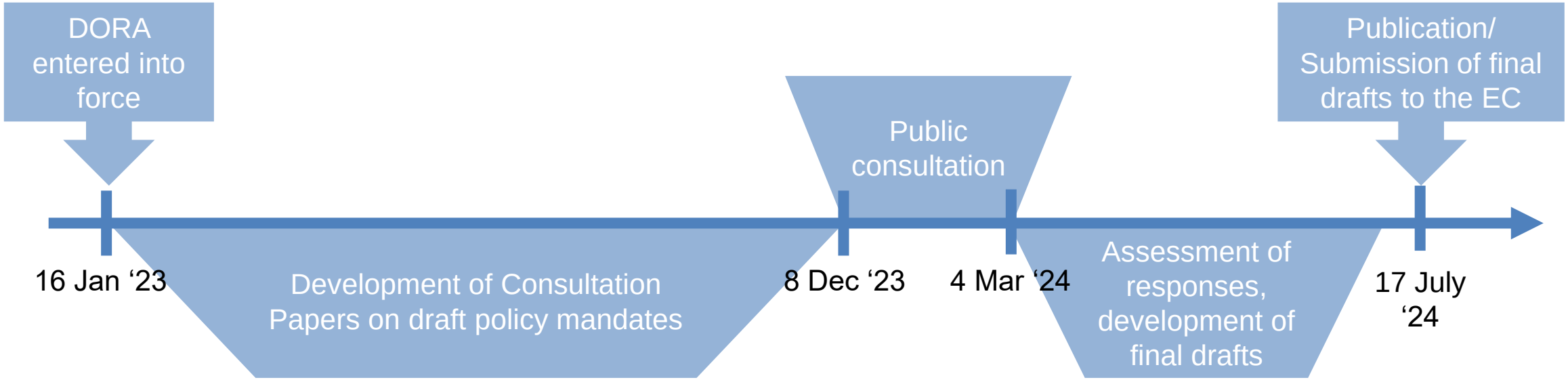
ESMA European Securities and Markets Authority

Purpose of the public hearing

The ESAs organise 'public hearings' for its Technical Standards and Guidelines to allow interested parties to ask clarification questions.

- The purpose of the hearing is for the ESAs to present a summary of the Consultation papers (CPs), reproduce the questions of the CP, and ask attendees whether they require additional explanations or clarifications from ESA staff to be able to answer the questions in the CP.
- The public hearing does, therefore, not replace written responses to the CP, as it is only through written responses that the ESAs are able to give the views of stakeholders the required consideration.
- The slides presented today will be shared on the ESAs websites after the event.

Timeline of the second batch of policy mandates



SESSION 1: RTS on oversight harmonisation

Andrea Vetrone – Senior Expert, EIOPA
Andra Remeur – Expert, EIOPA

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Key features of DORA oversight framework (Art. 31-44)

Objectives

- Strengthen the digital operational resilience of financial entities relying on critical ICT third-party service providers (CTPPs) to preserve the financial stability and the integrity of the internal market for financial services.
- Promote convergence and efficiency on supervisory approaches when addressing ICT third–party risks in the financial sector.

Key Features

- ESAs to assess if CTPPs have in place adequate processes to manage the risks they may pose to financial entities (FEs)
- Lead Overseer (LO) can issue recommendations to the CTPPs following general investigations or onsite inspections. The CTPP is not obliged by law to comply.
- Competent authorities (CAs) may require the FEs they supervise to take measures to address the risks related to the recommendations.
- ESAs and CAs to cooperate closely in the designation and day-to-day oversight of the CTTPs.

Overview of the mandate

- According to the mandate (Article 41(1)), the RTS shall specify:
  a) the information to be provided by an ICT third–party service provider in the application for a voluntary request to be designated as critical;
  b) the information to be submitted by the ICT third–party service providers that is necessary for the Lead Overseer (LO) to carry out its duties;
  c) the criteria for determining the composition of the joint examination team, their designation, tasks, and working arrangements;
  d) the details of the competent authorities' assessment of the measures taken by CTPPs based on the recommendations of the LO.
- On the basis of the specific nature of the empowerment, the ESAs decided to divide the mandate in two separate RTS :
  – one focusing on the areas of the mandate having a direct impact on financial entities and ICT third party service providers (points (a), (b) and (d) above). *Focus of today.*
  – the other one on the requirements to be followed by the competent authorities in relation to the joint examination team (point (c) above).
- The RTS covering point (c) will be publicly consulted from mid-April for one month (tentative schedule).

Structure of the RTS

Chapter 1 Opt-in information	Article 1 - Information to be provided by ICT third-party service providers in the application for a voluntary request to be designated as critical Article 2 - Assessment of completeness of application
Chapter 2 Info from CTPPs to LO	Article 3 - Content of information provided by critical ICT third-party service providers Article 4 - Remediation plan and progress reports Article 5 - Structure and format of information provided by critical ICT third-party service providers Article 6 Information on subcontracting arrangements provided by critical ICT third-party service providers
Chapter 3 CAs assessment of LO's recommendations	Article 7 - Competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer

Principles followed while developing the RTS

The primary goal of the draft RTS is to instore efficient oversight conditions vis-à-vis CTPPs, FEs, and CAs across the Union to avoid legislative fragmentation while ensuring the stability of the financial sector.

Chapter 1
Opt-in information

- An ICT provider submitting a voluntary opt-in request to the ESAs shall fill it in with the objective to demonstrate its criticality to the ESAs.
- A complete application contains all the information included in Article 1 of the RTS and only complete applications can be used to assess the criticality of an ICT provider opting in.

Chapter 2
Info from CTPPs to LO

- Information provided by the CTPPs should relate to the minimum required topics covered by the LO's assessment and it should be an open list of information as it allows for flexibility and adaptation since new trends and topics may emerge.
- To ensure an effective monitoring of actions/remedies relating to the recommendations, the CTPPs share (upon LO request): (i) interim and (ii) final reports on those actions/remedies with the LO.
- Information shall be provided according to the structure and in the format indicated by the LO.
- Reporting on CTTP' sub-contracting are based (but do not mirror) the requirements for FEs in the ITS on the register of information developed according to Art. 28(10).

Chapter 3
CAs assessment of LO's recommendations

- CAs monitor and assess the extent to which the FEs are exposed to the risks identified in the LO's recommendations, while the LO monitors and assesses the implementation by the CTPPs of actions and remedies to comply with them.
- CAs and LO should share information useful to achieve their respective tasks. When asking information to the CAs about their assessment of the exposure of the FEs to the risks identified in the recommendations, the LO should consider that the objective of the request is to evaluate the actions and remedies of the CTPPs.

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Opt-in information (Article 1)

- General information on the ICT third party service provider opting-in, including on its corporate structure and market share of the service provider in the financial sector (points (a) to (e))
- Clear description of the ICT services provided and of the financial entities receiving services, including, where available, information on the type of functions of the financial entities supported and if the latter are critical (points (f) and (g))
- Link with already designated CTPPs, both as customers and service providers to the ICT third-party service provider opting-in (points (h) and (k))
- A self-assessment of criticality covering (i) the degree of substitutability (considering: mkt share, nr. of competitors, specificities of services offered) and (ii) knowledge of alternative ICT TPPs providing similar ICT services (point (i))
- Information on future strategy and investment plans relating to the ICT services and infrastructure provided and in relation to the corporate or management structure (point (j)
- If the ICT third party service provider opting-in is part of a group, the information should refer to the ICT services provided by the group as a whole (Art. 1.2)

Information to be provided by CTPPs (Article 3.2)

- Information relating to the arrangements between CTPPs and FEs and CTPPs and their subcontractors (point (a))
- Organisational structure, major shareholders, market share per type of service and internal governance arrangements of the CTPPs (points (b) to (e)
- Meeting minutes of the management body and other internal relevant committees (point (f)
- Information on the following frameworks: (i) ICT security and data protection, (ii) risk management* (ii) incident management*, (iii) change management* (iv) response and recovery, (v) ICT third-party management. ,(points (g), (l), (m), (o)
- Information about measures taken by the CTPPs to address risks arising from the provision of ICT services by the CTPPs or their subcontractors (point k)
- Information about performance monitoring, security monitoring, incident tracking, reporting mechanisms relating to service performance, incidents and compliance to SLAs between CTPPs and FEs (point (n)
- Offering to their customers in relation to data portability, application portability and interoperability ,(point (h)
- Exact locations of data centres and production centres in EU and outside EU and information about service provision from third countries including relevant legal provisions (points (i) and (j)

* Relating to both the CTPPs and their subcontractors

Information to be provided by CTPPs (Article 3.2) *cont.*

- Extractions from monitoring and scanning systems and from production pre-production and test systems of the CTPPs or their subcontractors (points (p) and (q)
- Compliance and audit reports or certifications relating to the CTPPs or their subcontractors (point (r)
- Information about assessments evaluating the suitability and integrity of individuals holding key positions within the CTPPs (point s)
- Information about the remediation plan to address the recommendations issued by the LO (point t)
- information about employee training schemes and security awareness programs of the CTPPs staff (point u)
- Information about the activities of the CTPPs and financial statements, including information on the budget and resources related to ICT and security (point v)
- Other relevant information needed by the LO to monitor the provision of the ICT services provided by the CTPPs and to carry out its oversight duties in accordance with the requirements of DORA (point w)

Remediation plan and progress reports (Article 4)

- The CTPPs shall provide to the LO:
  - A remediation plan outlining actions/to mitigate the risks identified in the recommendations.

    The remediation plan shall be provided when the CTPP notifies its intention to follow the LO recommendation and be consistent with the timeline indicated by the LO.
  - Interim progress reports (and supporting documents).
  - Final reports (and supporting documents).

Structure and format of the information (Article 5)

- CTPPs shall:
  - provide the requested information to the LO through the secure electronic channels indicated by the LO in its request.
  - Follow the structure indicated by the LO in the information request.
  - provide a clear indication of where the requested documentation can be found.

Information on subcontracting (Article 6 and Annex I)

- The CTPPs shall provide to the LO information on subcontracting arrangements belonging to the following dimensions:
  - General information on the reporting CTPP (e.g. name, LEI)
  - Overview of subcontracting arrangements (e.g. type of ICT services performed by subcontractors and mapping of the arrangements)
  - General information on subcontractors (e.g. name, LEI, contact person, expertise and knowledge in the field of contracted services)
  - Description of the services provided by subcontractors
  - Risk management and compliance (e.g. CTPP's risk assessment on subcontractors)
  - Business continuity and contingency planning
  - Description of the reporting mechanisms
  - Remediation and incident management
  - Certifications and audits

Questions for consultation

1. Do you agree with the content of information to be provided by ICT third party providers in the application for a voluntary request to be designated as critical? (Article 1)

2. Is the process to assess the completeness of opt-in application clear and understandable? (Article 2)

3. Is the list of information to be provided by critical ICT third-party service providers to the Lead Overseer that is necessary to carry out its duties clear and complete? (Article 3)

4. Do you agree with the content of Article 4 on remediation plan and progress reports?

5. Is the article on the structure and format of information provided by the critical ICT third-party service provider appropriate and structured? (Article 5)

6. Is the information to be provided by the critical ICT third-party service provider to the Lead Overseer complete, appropriate and structured? (Article 6 and Annex I)

7. Is Article 7 on competent authorities' assessment of the risks addressed in the recommendations of the Lead Overseer clear?

8. Do you agree with the impact assessment and the main conclusions stemming from it?

SESSION 2: Guidelines on oversight cooperation

Andrea Vetrone - Senior Expert, EIOPA

Overview and scope of the mandate

- Article 32(7) mandates the ESAs to issue guidelines on the cooperation between the ESAs and CAs covering:
  - the detailed procedures and conditions for the allocation and execution of tasks between competent authorities and the ESAs; and
  - the details on the exchanges of information which are necessary for competent authorities to ensure the follow–up of recommendations according to Article 35(1), point (d), addressed to critical ICT third–party service provider.
- The guidelines cover the articles 31 to 44 of DORA (chapter V – Section II oversight framework)

  Excluded from the scope of the guidelines:
  - Articles and tasks applying only to CAs or ESAs (e.g. art 43 on oversight fees)
  - Articles and tasks applying only to FEs or CTPPs (e.g. Art. 35(5) on CTTP's cooperation with LO in good faith)
  - Cooperation ESAs-CAs in the context of Oversight Forum or Joint Oversight Network
  - Aspects relating to the criteria to designate CTPPs or the composition of the joint examination teams

Structure of the Guidelines

The primary goal of the draft guidelines is to achieve efficient and effective cooperation between the actors in the supervisory community and to ensure that information is shared transparently on a need-to-know basis with the objective to ensure timely and successful results of the oversight framework.

General considerations Guidelines 1 to 4	Language, contact points, communication means and resolution of divergence of opinions.
Designation of CTPPs Guidelines 5 and 6	Information exchange between LO, CAs and OF in the context of CTPPs designation.
Oversight activities Guidelines 7 to 10	Procedures and information exchanges in relation to: (i)oversight plan; (ii) general investigations; (iii) inspections (iv) measures concerning CTPPs taken by CAs in agreement with the LO.
Follow-up of recommendations Guidelines 11 to 13	General principles and information exchanges including in case of CAs decision to require FEs to suspend/terminate contracts with CTPPs.
Final provisions	Application date and review clause 4 years after publication.

Overview of the guidelines

Guideline 1 Language, communication means, contact points and accessibility	In addition to the definition of English as standard language for communication and the need to nominate contact points, the GL introduces the obligation for the ESAs to implement an online tool to ensure the secure and confidential sharing of information between ESAs and CAs.
Guideline 2 Timelines	The specific timelines set in the guidelines can be adjusted by the LO in consultation with CAs.
Guideline 3 Difference of opinion between ESAs and CAs	In case where no mutually agreed solution is reached, LO should present the different of opinions of CAs and ESAs to the OF which will present its view to find a mutually agreed solution.
Guideline 4 Info exchange between ESAs and CAs with NIS Authorities	Where possible, CAs and ESAs should share information stemming from their dialogue with NIS authorities.
Guideline 5 Info for the criticality assessment submitted by CAs to the OF	CAs should transmit to the OF: (i) the full register of information (ii) info at CAs disposal to facilitate the criticality assessment.
Guideline 6 Info on CTPPs designation submitted by ESAs to CAs	ESAs should transmit to the CAs: (i) general info on the CTPPs (ii) changes to the structure of the management of the subsidiary in the EU ex Art. 31(13); (iii) starting date of oversight.

Overview of the guidelines

Guideline 7 Annual oversight plan	LO to share oversight plan and its updates to relevant CAs including info on: (i) type of oversight activity; (ii) high-level scope and objectives; (iii) timeframe; (iv) FTEs needed; (v) staff profile.
Guideline 8 General investigation & inspection	LO to inform relevant CAs of the identity of authorised persons for the general investigation or inspection.
Guideline 9 Measures by CAs concerning CTPPs	Process to share info and obtain LO agreement on planned (shared after receiving oversight plan) and ad hoc measures concerning CTPPs.
Guideline 10 Additional info exchange between LO and CAs	LO to share to relevant CAs: (i) scope of the request for information submitted to CTPPs; (ii) major ICT related incident reported by the CTPPs to the LO; (iii) changes in the ICT third-party risk management strategy of the CTPP; (iv) important risks to the provisioning of ICT services; (v) reasoned statement by CTPP on the oversight plan. If a CTPP liaise with CAs in relation to oversight, CAs to share with LO content of these exchanges.
Guideline 11 General principles for follow-up	CAs: (i) PoC for FEs (ii) responsible to follow-up risks identified in LO's recommendations with FEs. LO: (i) PoC for CTPPs (ii) responsible to follow-up LO's recommendations with CTPPs.

Overview of the guidelines

Guideline 12

Info exchanges to ensure follow up of recommendations

LO to share to relevant CAs: (i) notification of CTPP to follow LO's recommendations; (ii) reasoned explanation of the CTPP for not following LO's recommendations and the related LO's assessment; (iii) progress reports and the related LO assessment; (iv) decision to impose a periodic penalty payment (v) failure of the CTPP to send the notification after issuance of recommendations.

CAs to share with LO in case CTPPs do not endorse LO's recommendations: (i) notification to FEs in case CAs believes the FEs do not consider or sufficiently address the risks in LO's recommendations; (ii) individual warnings issued according to Art. 42(7); (iii) outcome of the consultation with NIS Authorities ex Art. 42(5); (iii) changes to FEs' arrangements with CTPPs to address the risks in LO's recommendation and (iv) start of execution of exit strategies from CTPPs by FEs.

GL 12 provides also cases when LO's recommendations are considered not endorsed by CTPPs

Guideline 13

Decision to FEs to suspend / terminate a service / contract with a CTPP

1) CAs to inform LO intention to notify a FE of the possibility of a CA decision if the FE does not adopt contractual arrangements to address risks included in the recommendation ex Art. 42(4).
2) LO to assess the impact of that decision on the concerned CTPP
3) In case two or more CAs plan (or have) to take a decision sub 1, LO should inform about inconsistent supervisory approaches that could lead to an unlevel playing field.

Questions for consultation

1. For each guideline, do you consider the Guideline to be clear, concise and comprehensible?
2. Taking into account the specific scope of these Guidelines, do you consider that these Guidelines cover all the instances where cooperation and information exchange between CAs and the LO is necessary?
3. Do you consider that the implementation of these Guidelines will contribute to adequate cooperation and information exchange between the ESAs and CAs in the conduct of oversight activities?
4. What are your main expectations regarding the impact on financial entities and CTPPs of the application of these Guidelines?

SESSION 3: RTS and ITS on major incident reporting

Antonio Barzachki - Senior policy expert, EBA

Background

DORA has introduced a harmonised and streamlined framework for reporting of major ICT-relates incidents where FEs

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

Major ICT-related incidents are classified based on six criteria set out in DORA

- Clients, financial counterparts or transactions affected and reputational impact
- Duration and service downtime
- Geographical spread
- Data losses
- Criticality of the services affected
- Economic impact

RTS on criteria for classification of major ICT-related incidents and significant cyber threats (under Art. 18(3) DORA)

Developed and published on 17 January 2024. The RTS specifies the criteria and their thresholds for major ICT-related incidents; the criteria and materiality thresholds for determining significant cyber threats, the criteria for competent authorities to assess relevance of the incident to other Member States and the details to be shared with other competent authorities.

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Overview of the legal mandates conferred on the ESAs

Article 20(a)

RTS on the content and timelines for reporting major ICT-related incidents and significant cyber threats

The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall develop common draft RTS 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**.

*The ESAs shall take into account the **proportionality** criteria set out in Article 20 DORA and be **consistent** with the approach* for incident reporting under Directive (EU) 2022/2555 (**NIS2**).

Article 20(b)

ITS on the forms, templates and procedures for reporting major ICT-related incidents and significant cyber threats

*The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall develop common draft ITS in order to establish the **standard forms, templates and procedures** for financial entities to report a major ICT-related incident and to notify a significant cyber threat.*

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Time limits for reporting major ICT-related incidents (RTS)

Initial notification

- As soon as possible within 4 hours from classification of the incident
- No later than 24 hours from detection of the incident

Intermediate report

The earliest between:

- 72 hours from the classification of the incident as major (Art. 6(1)(b) of the RTS)
- when regular activities have been recovered and business is back to normal (Art. 6(1)(b) RTS)
- as soon as the status of the original incident has changed significantly (Art. 19.4 DORA)
- when the handling of the incident has changed based on new information (Art. 19.4 DORA)

Submit a revised intermediate report if status update available or upon request from competent authority

Final report

- No later than 1 month from classification of the incident
- The day after the incident is fully resolved

Where the submission deadline of an intermediate or final report falls on a weekend/bank holiday, FEs may submit the report in the first hour of the next working day, unless the incident has cross-border impact, the FE is a significant institution, systemic at national level or a financial market infrastructure.

Content of the major incident notification/reports (RTS&ITS)

General information

- Type of report
- Name, type and LEI code of the reporting and/or affected financial entity
- Contact details of responsible persons within the affected financial entity or a third-party reporting
- Identification of the parent undertaking of the group, where applicable; and Reporting currency

Initial notification

- Date and time of detection and classification of the incident
- Description of the incident and information on its origin
- Classification criteria met
- Impact in other Members States or to other financial entities and/or third-party providers
- Information whether the incident is recurring; indication of activation of business continuity plan

Intermediate report

- Type of the incident
- Information about the classification and thresholds that trigger the incident report
- Discovery of the incident and whether the incident originates from a third-party provider or another financial entity
- Information about affected functional areas, business processes and infrastructure components
- Communication to clients and/or financial counterparts or reporting to other authorities, where applicable;
- Temporary actions/measures taken to recover from the incident
- Information on vulnerabilities exploited and indicators of compromise, where applicable
- Others

Content of the major incident notification/reports (RTS&ITS)

Final report

- Date and time when the incident was resolved permanently
- Information about the root cause of the incident
- Information about direct and indirect costs and losses stemming from the incident and financial recoveries
- Information about inability to comply with legal requirements or breach of contractual arrangements
- Information on the measures/actions taken for the incident resolution and additional controls to prevent similar incidents in the future
- Information relevant for resolution authorities
- Others

Rationale behind the proposed data fields to be included in the reporting requirements

- Competent authorities to collect all essential information about the major ICT-related incidents
- Financial entities to not face unnecessary reporting burden
- The information collected to be useful for NIS2 and resolution authorities (due to *lex specialis* nature of DORA)

	Mandatory fields	Conditional fields
General information	10	8
Initial notification	9	8
Intermediate report	15	24
Final report	12	15
TOTAL	46	55

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Content of notifications for significant cyber threats (RTS&ITS)

Main aspects & rationale

- Voluntary reporting of significant cyber threats as stipulated in DORA
- Simple and concise content avoiding burden for FEs and encouraging reporting
- Leverage on data fields used for incident reporting but reflecting specificities of cyber threats

Information requested

- General information about the financial entity
- Date and time of detection of the cyber threat
- Description of the significant cyber threat
- Information about potential impact
- Potential incident classification criteria
- Status of the cyber threat
- Actions taken to prevent materialisation
- Notification to other stakeholders
- Indicators of compromise

Format, templates and reporting requirements (ITS)

Template

- A single template covering the initial notification, intermediate and final incident reports
- Description of each field and instruction to populate included in the template
- Flexibility to populate fields in subsequent reports or updates to preceding submissions
- Proportionate (essential fields only, mandatory and conditional fields)
- Aggregated reporting potentially possible at national level, subject to an agreement with the relevant competent authority
- Specific reporting template for significant cyber threats

Reporting requirements

- Reporting at financial entity (solo) level only
- Requirements are technology neutral – no preference for any specific reporting solution
- Reporting channels should be secured and agreed with the competent authority
- In case of inability to submit a notification/report, financial entities shall inform competent authorities within 24 hours
- Standard prudential reporting approach with requirements ensuring completeness and accuracy of information
- Outsourcing – financial entities to inform their competent authority of name and contact details, including LEI code, of the third-party provider.

Overview of the questions asked

Question 1 – Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

Question 2 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 3 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 4 – Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA? If not, please provide your reasoning and suggested changes.

Question 5 – Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA? If not, please provide your reasoning and suggested changes.

Question 6 – Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

Lunch break – meeting will restart at 14:00

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

SESSION 4: Guidelines on cost and losses caused by major ICT-related incidents

Christoph Erkunt (Expert, EBA)

Overview of the legal mandates conferred on the ESAs

Mandate for the ESAs on developing GL

- In accordance with Article 11(10) DORA, CAs may request from a financial entity an estimation of aggregated annual costs and losses caused by major ICT-related incidents
- Article 11(11) DORA mandates ESAs to develop common guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents'

Approach taken by the ESAs for developing the Guidelines

- Identical delineation of costs, losses and financial recoveries with the other Technical Standards on incident classification and on incident reporting
- Alignment with the operational risk framework for credit institutions
- Avoid posing reporting burden to financial entities

Key elements of the Guidelines

Delineation of the relevant reference period for the 'annual' aggregated costs and losses

- Set the completed accounting year as reference period and only account for those costs and losses that fall within that period
- Use as far as possible validated financial statements for that year as data source

  This aims at not posing reporting burden to financial entities as they can take the numbers from their regular accounting

Specification which ICT-related incidents to include within a given year

Only those that have been classified as major, and

- For which the financial entity submitted a final report in the reference period, or
- For which the financial entity submitted a final report in previous accounting years but that the incident had a financial impact in the reference period

Key elements of the Guidelines

Step-by-step description how to estimate the 'aggregated' costs and losses

- Sum up for the relevant incidents all costs and losses within the reference period
- Use definitions of costs, losses and recoveries provided in the RTS on incident classification and the ITS on incident reporting of major ICT-related incidents
- Include adjustments to calculations from previous years in the calculation of the reference period

Description of the reporting obligations and template

- The reporting should include the annual aggregated gross costs, recoveries and net costs
- The reporting should also include the breakdown of the gross costs, recoveries and net costs by major ICT-related incident

Overview of the questions asked

Question 1 – Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

Question 2 – Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

Question 3 – Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents? If not, please provide your reasoning and alternative approach(es) you would suggest.

SESSION 5: RTS to specify the elements to determine and assess when sub-contracting ICT services supporting critical or important functions

Djamel Bouzemarene - Senior policy expert, EBA

Overview of the mandate

- According to the mandate (Article 30(5)), the RTS shall specify further the elements referred to in Article 30(2) point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.
- In accordance with Article 30(2) (a) of DORA, the contractual arrangements on the use of ICT services shall include 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.

Structure of the RTS

The structure of the RTS follows the life-cycle of arrangements regarding the use of ICT TPSPs when subcontracting ICT services

General considerations	Article 1 - Complexity and risk considerations Article 2 – Group application
Pre-contractual phase	Article 3 - Risk assessment regarding the use of subcontractors
Contractual phase	Article 4 - Description and conditions under which ICT services supporting a critical or important function may be subcontracted
Monitoring phase	Article 5 - Monitoring of the entire ICT subcontracting chain by the financial entity Article 6 - Material changes to subcontracting arrangements
Exit phase	Article 7 - Termination of the contractual arrangement

Summary of the subcontracting requirements through the subcontracting arrangements life-cycle

Pre phase	Contractual phase	Monitoring	Exit
<< Elements of increased or reduced risks >>			
Risk assessment by FE before subcontracting • Due diligence by TPSP • Compliance with FE's legal requirements under DORA • Impact of failure • Concentration risks Periodical assessment against material changes	Conditions for subcontracting • Monitoring and reporting by TPSP • Subcontractor reporting towards TPSP, and FE if appropriate • Risk assessment of location by TPSP • BCP • ICT security • Audit and access rights	• FE to document full subcontracting chain (RTS on register) • Monitoring of full subcontracting chain by FE • Assessment of KPIs against contractual conditions • Material changes lead to information and reassessment	FE has right to terminate agreement with TPSP in case of • Subcontracting not permitted by agreement • Material changes despite objection or without information Fallback actions fall under the scope of the RTS in ICT policy

Questions for consultation

1. Are the considerations on complexity and risk, and group application, appropriate and sufficiently clear? (Articles 1 and 2)
2. Is the risk assessment regarding the use of subcontractors appropriate and sufficiently clear? (Article 3)
3. Are the conditions under which ICT services supporting a critical or important function may be subcontracted appropriate and sufficiently clear ? (Article 4)
4. Are the monitoring requirements appropriate and sufficiently clear? (Article 5)
5. Are the information and re-assessment requirements triggered by material changes to subcontracting, and the termination rights appropriate and sufficiently clear ? (Articles 6 and 7)

SESSION 6: RTS on TLPT

Karole-Anne Sauvet-Frot - Senior Policy Officer, ESMA

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Agenda

- **The DORA TLPT RTS and the TIBER-EU framework**
- **Overview of the RTS mandate**
- **Drafting approach**
- **Structure of the proposed draft RTS**
- **Proposed draft RTS: main features**
  1. Identification of financial entities required to perform TLPT
  2. Testing process
  3. Use of internal testers
  4. Cooperation

The DORA TLPT RTS and the TIBER-EU framework

- Threat-led penetration testing (TLPT)' means a framework that **mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems**. DORA, Article 3(17)

- Article 26(11) of DORA mandates the ESAs in agreement with the ECB to develop RTS **in accordance with the TIBER-EU framework** to specify further certain aspects of a threat-led penetration testing (TLPT) framework under DORA

The ECB TIBER-EU framework

- A TLPT framework inspired from national standards (UK, NL)
- Jointly developed by the ECB and the national central banks
- Published in 2018, and already adopted by 14 Member States

Overview of the RTS mandate

DORA Level 1

DORA Chapter IV - Digital operational resilience testing

- Article 24 - General requirements
- Article 25 - Testing of ICT tools and systems
- Article 26 - Advanced testing of ICT tools, systems and processes based on TLPT
- Article 27 - Requirements for testers for the carrying out of TLPT

Level 2 RTS mandate

DORA Article 26(11)

- (a) Criteria to select financial entities
- (b) Use of internal testers
- (c) Scope Testing process Results
- (d) Cooperation when financial entities operate in more than 1 MS

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

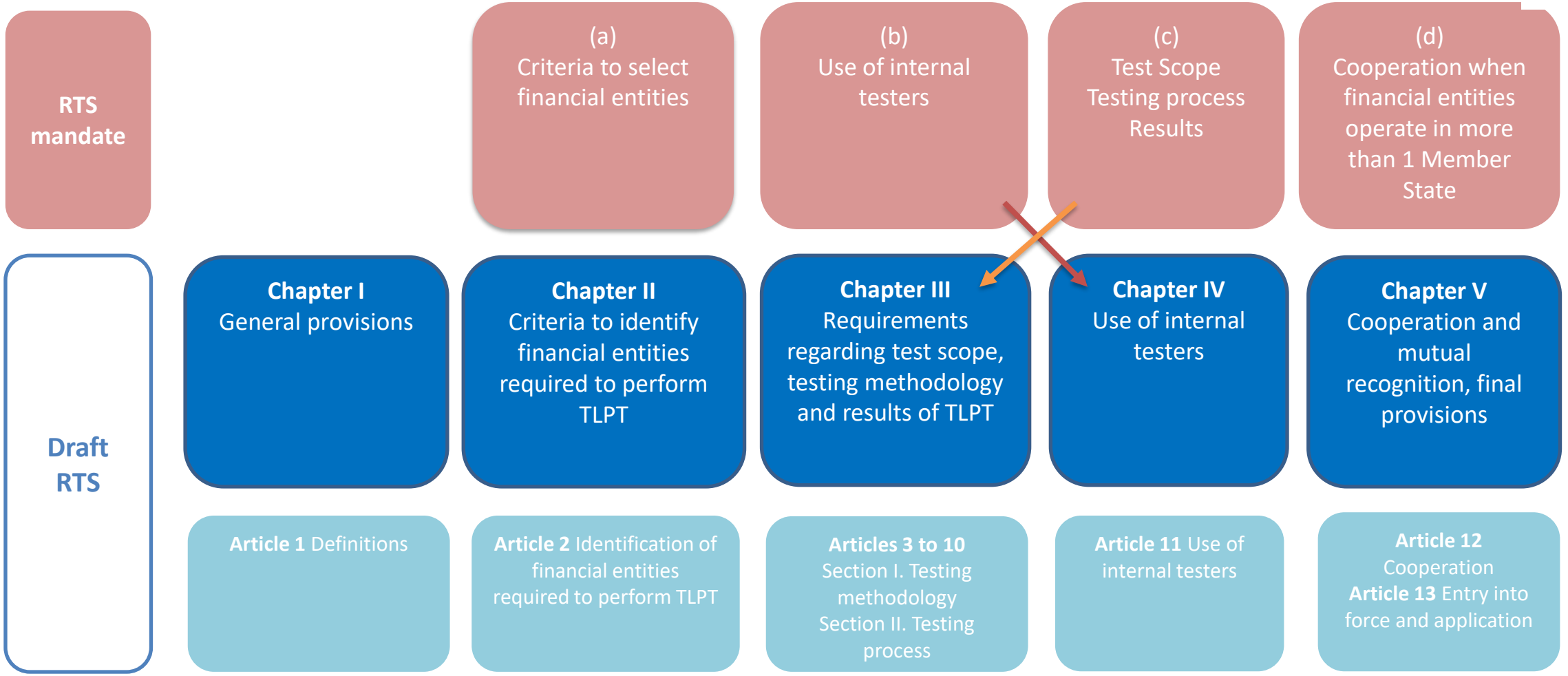
Drafting approach

- **L1** already includes provisions on:

- Based on L1, **incorporation of as much as possible of the TIBER-EU Framework**

- Main **differences**:
  - Authority responsible for TLPT
  - Testers
  - Purple teaming

Structure of the proposed draft RTS



Proposed draft RTS

1 – Identification of financial entities

DORA
3 criteria

Draft RTS

By default
with opt out possible on case-by-case basis

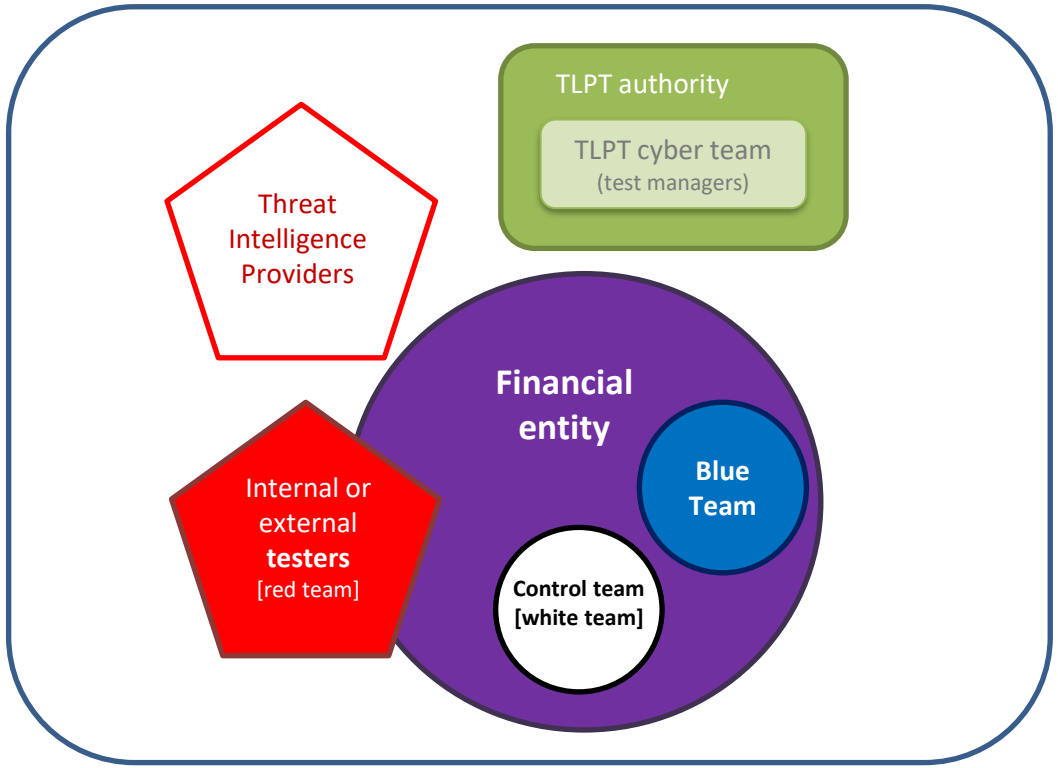
- Significant credit institutions above certain thresholds
- Payment institutions above certain thresholds
- Electronic money institutions above certain thresholds
- CSDs
- CCPs
- Trading venues above certain thresholds
- Insurance/reinsurance undertakings above certain thresholds

On a case-by-case basis
based on an assessment of the criteria

All other financial entities

Proposed draft RTS
2 – Testing process (1/2)

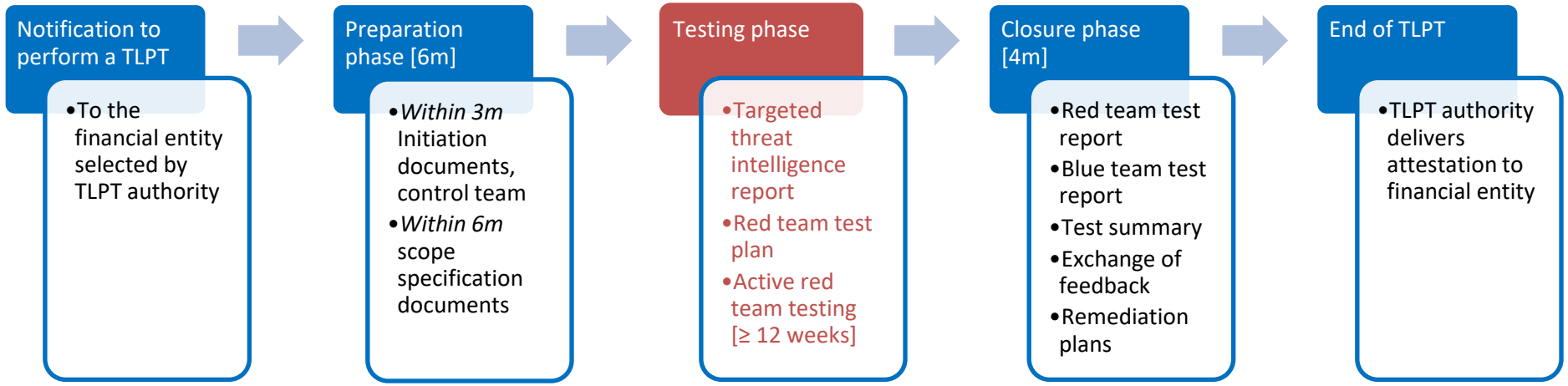
- **Parties involved**



- **Organisational arrangements**: appointment of control team and ensuring security of the financial entity and the secrecy of TLPT
- **Risk management measures** by control team: requirements for testers and threat intelligence provider in particular on minimum experience (based on TIBER-EU services procurement guidelines)

Proposed draft RTS
2 – Testing process (2/2)

- **Timeline** (simplified)



- **TLPT authority** validates documents, choice of testers and changes to process
- **Meetings** recommended at each stage of the process
- Specificities for **pooled testing**: TLPT authority of the designated FE to lead, remediation plan at the level of each FE

Proposed draft RTS
3 – Use of internal testers

DORA requirements for **all** testers

Art 27(1)

- Suitability, reputability
- Specific expertise in TI, PT and red team testing
- Certification or adherence to code of conduct
- Sound risk management for the FE
- Professional indemnity insurance

DORA additional requirements for **internal testers**

Art 26 (8)

External testers every 3 TLPT

No internal testers for SIs

Art 27(2)

- Approval by TLPT authority
- FE manages conflicts of interests
- External TI provider

Draft RTS additional requirements for internal testers

- FEs to define **policy** for the management of internal testers
- **No impact** on the FE defensive capabilities
- Testers to be given **sufficient resources** and capabilities
- TLPT authority to check **experience** before validating use (same as external testers and TI providers)

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Proposed draft RTS
4/ Cooperation

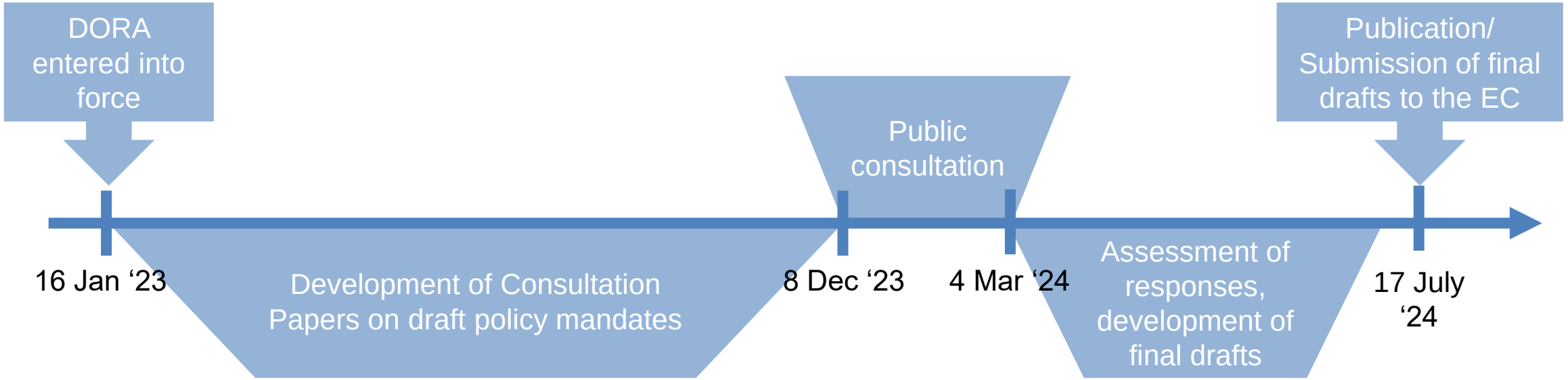
Cooperation between TLPT authorities **from different Member States** (MS): 2 cases

A financial entity providing services in at least 2 MS	• If critical functions are operated by the FE in different MS • TLPT authority of the FE to identify other relevant TLPT authorities • Various levels of **involvement** in the TLPT
Financial entities established in several MS and belonging to the same **group**	• Possibility to conduct **joint TLPTs** on these financial entities • TLPT authorities to agree on who will lead the TLPT

Questions for consultation

General approach	Q1. Do you agree with this cross-sectoral approach? If not, please provide detailed justifications and alternative wording as r Q2. Do you agree with this approach on proportionality? If not, please provide detailed justifications and alternative wording as needed.
Criteria to select FEs	Q3. Do you agree with the two-layered approach proposed to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed. Q4. Do you agree with the proposed quantitative criteria and thresholds in Article 2(1) of the draft RTS to identify financial entities required to perform TLPT? If not, please provide detailed justifications and alternative wording as needed.
Testing process	Q5. Do you consider that the RTS should include additional aspects of the TIBER process? If so, please provide suggestions. Q6. Do you agree with the approach followed for financial entities to assess the risks stemming from the conduct of testing by means of TLPT? If not, please provide detailed justifications and alternative wording as needed. Q7. Do you consider the proposed additional requirements for external testers and threat intelligence providers are appropriate? If not, please provide detailed justifications and alternative wording or thresholds as needed. Q8. Do you think that the specified number of years of experience for external testers and threat intelligence providers is an appropriate measure to ensure external testers and threat intelligence providers of highest suitability and reputability and the appropriate knowledge and skills? If not, please provide detailed justifications and alternative wording as needed. Q9. Do you consider the proposed process is appropriate? If not, please provide detailed justifications and alternative wording as needed. Q10. Do you consider the proposed requirements for pooled testing are appropriate? If not, please provide detailed justifications and alternative wording as needed.
Internal testers	Q11. Do you agree with the proposed requirements on the use of internal testers? If not, please provide detailed justifications and alternative wording as needed.
Cooperation	Q12. Do you consider the proposed requirements on supervisory cooperation are appropriate? If not, please provide detailed comments and alternative wording as needed.
Any other comments	Q13. Do you have any other comment or suggestion to make in relation to the proposed draft RTS? If so, please provide detailed justifications and alternative wording as needed.

Timeline of the second batch of policy mandates



Annex

Q&A on Regulation

- The objective of ESAs Question and Answer process on regulation (Q&A process) is to ensure consistent and effective application of European regulation and to foster supervisory convergence in the EEA within the ESAs respective scope of action, including DORA.
- Any natural or legal person, including financial institutions, competent authorities and Union institutions and bodies can use the Q&A process for submitting questions relating to the practical application or implementation of the applicable laws, regulations and guidelines.
  - EBA's Questions and Answers (europa.eu)
  - EIOPA's Questions and Answers (europa.eu)
  - ESMA's Questions and Answers (europa.eu)