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

13 July 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

Programme

- **09.00 – 09:10 Opening of the conference**
- **09:10-09:20 Welcoming remarks**

  José-Manuel Campa (Chairperson, EBA)
- **09.20 – 09.35 Keynote speech**

  Gerry Cross (Chairperson, Joint Committee Sub-Committee on Digital Operational Resilience)
- **09.35 – 11:35 SESSION 1: RTS on ICT risk management framework and RTS on simplified ICT risk management framework**

  Barbara Daskala (Senior Supervision Officer, ESMA)
- **11.35 – 11:45 Coffee break**
- **11:45. – 13.00 SESSION 2: RTS to specify the policy on ICT services performed by ICT third-party providers**

  Francesco Mauro (Head of Unit, EBA)
- **13.00 – 14.00 Lunch break**
- **14:00. – 16.00 SESSION 3: RTS on criteria for the classification of ICT-related incidents**

  Antonio Barzachki (Senior Policy expert, EBA)
- **16:00 – 16:15 Coffee break**
- **16.15 – 18.00 SESSION 4: ITS to establish the templates for the register of information**

  Andrea Vetrone (Senior Expert on Supervisory Oversight, EIOPA)
- **18.00 End of the meeting**

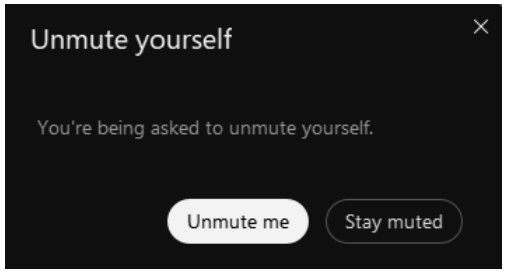
How to interact with us today: Slido

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

José-Manuel Campa, Chairperson of EBA

Keynote speech

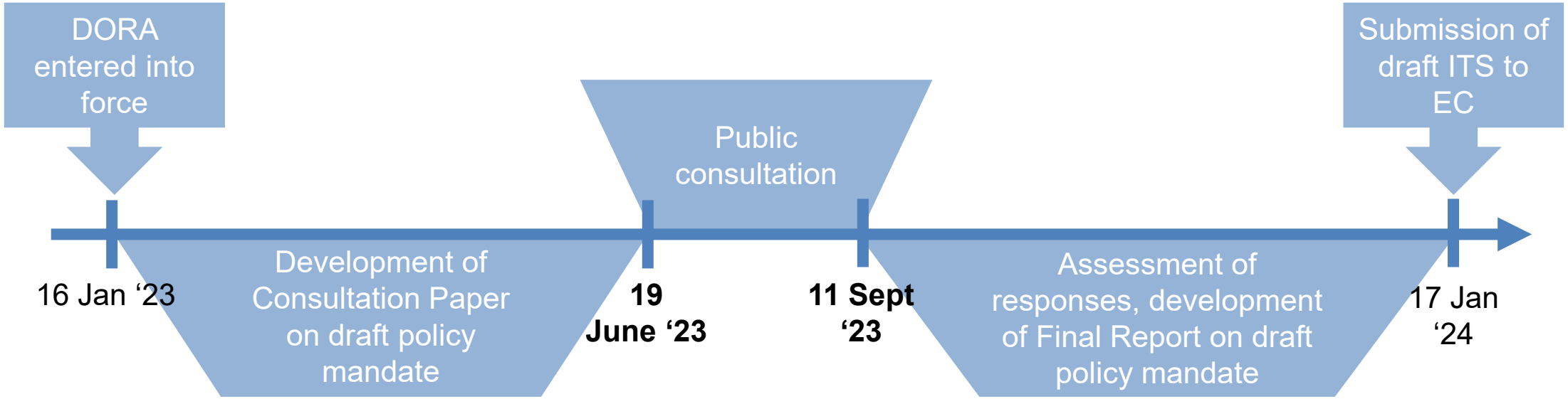
Gerry Cross, Chairperson of the Joint Committee sub-committee on Digital Operational Resilience

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 so as 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.

Timeline of the first batch policy development



SESSION 1: RTS on ICT risk management framework and RTS on simplified ICT risk management framework

Barbara Daskala, Senior Supervision Officer ESMA

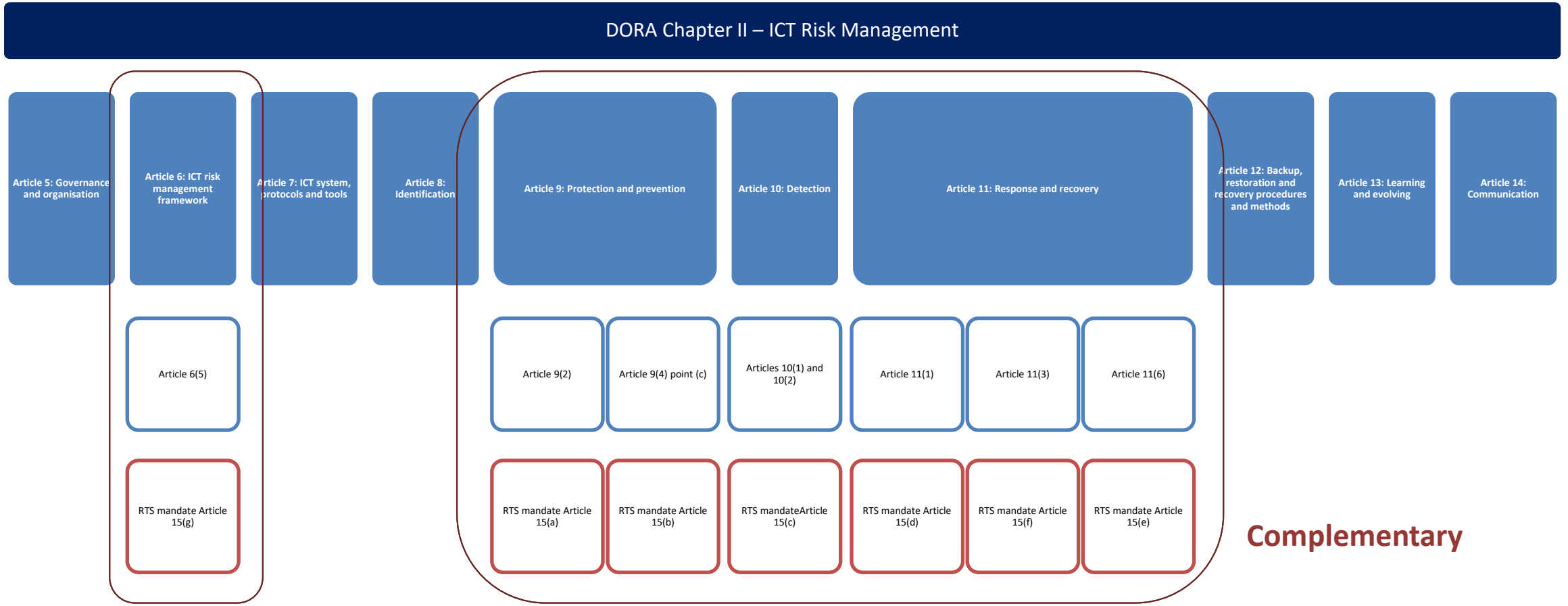
Overview of the ICT Risk Management Framework RTSs mandate

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)**

Principles followed for both RTSs

- Principle-based, to the extent possible
- Rule-based, as appropriate to cover detail required
- Technology-agnostic
- Proportionality
- Structure close to the mandate, but also…
- Considering existing industry leading practices and standards (e.g. ISO 27000)
- Scope differences between RTS of Article 15 and Article 16

DORA Chapter II (Articles 1 to 14) versus RTS 15



Overview of the RTSs (Titles I and I)

RTSs as mandated under Articles 15 and 16(3) of DORA

Title I Article 15					Title II Article 16 (3)
15(a)	15(b)	15(c)	15(d,e,f)	15(g)	
Chapter I: ICT security policies, procedures, protocols, and tools	**Chapter II**: Human resources policy and access control	**Chapter III**: ICT-related Incident detection and response	**Chapter IV**: ICT Business continuity management	**Chapter V**: Report on the ICT risk management framework review	**Chapter I:** Simplified ICT risk management framework

next slide

RTS 15 – Chapter I

Chapter I

ICT security policies, procedures, protocols and tools (Article 15a)

Section I	Section II	Section III	Section IV	Section V	Section VI	Section VII	Section VIII	Section IX
PROVISIONS ON GOVERNANCE	ICT RISK MANAGEMENT	ICT ASSET MANAGEMENT	ENCRYPTION AND CRYPTOGRAPHY	ICT OPERATIONS SECURITY	NETWORK SECURITY	ICT PROJECT AND CHANGE MANAGEMENT	PHYSICAL AND ENVIRONMENTAL SECURITY	ICT AND INFORMATION SECURITY AWARENESS AND TRAINING

RTS 16 – Overview

Title II Article 16 (3)

Simplified ICT Risk management framework

Chapter I	Chapter II	Chapter III	Chapter IV
ICT RISK MANAGEMENT FRAMEWORK	FURTHER ELEMENTS OF SYSTEMS, PROTOCOLS, AND TOOLS TO MINIMISE THE IMPACT OF ICT RISK	ICT BUSINESS CONTINUITY MANAGEMENT	REPORT ON THE REVIEW OF THE ICT RMF

PC Questions – RTS 15

General drafting principles	**Q1.**	Do you agree with the approach followed to incorporate proportionality in the RTS based on Article 15 of DORA (Title I of the proposed RTS) and in particular its Article 29 (Complexity and risks considerations)? If not, please provide detailed justifications and alternative wording as needed.
	Q2.	Do you agree with the approach followed for the RTS based on Article 16 of DORA (Title II of the proposed RTS)? If not, please provide an indication of further proportionality considerations, detailed justifications and alternative wording as needed.
Provisions on governance	**Q3.**	Do you agree with the suggested approach regarding the provisions on governance? If not, please explain and provide alternative suggestion as necessary.
ICT risk management	**Q4.**	Do you agree with the suggested approach on ICT risk management policy and process? If not, please explain and provide alternative suggestion.
ICT asset management	**Q5.**	Do you agree with the suggested approach on ICT asset management? If not, please explain and provide alternative suggestion.
	Q6.	Do you consider important for financial entities to keep record of the end date of the provider's support or the date of the extended support of ICT assets?
Encryption and cryptography	**Q7.**	Do you agree with the suggested approach on encryption and cryptography? If not, please explain and provide alternative suggestion.
	Q8.	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
ICT operations security	**Q9.**	Do you agree with the suggested approach on ICT operations security? If not, please explain and provide alternative suggestion.
	Q10.	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
	Q11.	What would be the impact on the financial entities to implement weekly automated vulnerability scans for all ICT assets, without considering their classification and overall risk profile? Please provide details and if possible, quantitative data.
	Q12.	Do you agree with the requirements already identified for cloud computing resources? Is there any additional measure or control that should be considered specifically for cloud computing resources in the RTS, beyond those already identified in Article 11(2) point (k)? If yes, please explain and provide examples.
Network security	**Q13.**	Do you agree with the suggested approach on network security? If not, please explain and provide alternative suggestions.
	Q14.	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.

PC Questions – RTS 15 *(cont'd)*

ICT project and change management	**Q15.**	Do you agree with the suggested approach on ICT project and change management? If not, please explain and provide alternative suggestions.
	Q16.	Do you consider that specific elements regarding supply-chain risk should be taken into consideration in the RTS? If yes, please explain and provide suggestions.
	Q17.	Do you agree with the specific approach proposed for CCPs and CSDs? If not, please explain and provide alternative suggestion.
Physical and environmental security	**Q18.**	Do you agree with the suggested approach on physical and environmental security? If not, please explain and provide alternative suggestions.
	Q19.	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
ICT and information security awareness and training	**Q20.**	Do you agree with the suggested approach regarding ICT and information security awareness and training? If not, please explain and provide alternative suggestions.
Human resources policy and access control	**Q21.**	Do you agree with the suggested approach on Chapter II - Human resources policy and access control? If not, please explain and provide alternative suggestion.
	Q22.	Is there any new measure or control that should be taken into consideration in the RTS in addition to those already identified? If yes, please explain and provide examples.
ICT-related incident detection and response	**Q23.**	Do you agree with the suggested approach regarding ICT-related incidents detection and response, in particular with respect to the criteria to trigger ICT-related incident detection and response process referred to in Article 24(5) of the proposed RTS? If not, please explain and provide alternative suggestion.
ICT business continuity management	**Q24.**	Do you agree with the suggested approach on ICT business continuity management? If not, please explain and provide alternative suggestion.
	Q25.	Do you agree with the suggested specific approach for CCPs, CSDs and trading venues? If not, please explain and provide alternative suggestion.
Report on the ICT risk management framework review	**Q26.**	Do you agree with the suggested approach on the format and content of the report on the ICT risk management framework review? If not, please explain and provide alternative suggestion.

PC Questions – RTS 16

Simplified ICT risk management framework	**Q27.**	Do you agree with the suggested approach regarding the simplified ICT risk management framework? If not, please explain and provide alternative drafting as necessary.
Further elements of systems, protocols, and tools to minimise the impact of ICT risk	**Q28.**	Do you agree with the suggested approach regarding the further elements of systems, protocols, and tools to minimise the impact of ICT risk under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.
	Q29.	What would be the impact for financial entities to expand the ICT operation security requirements for all ICT assets? Please provide details and if possible, quantitative data.
	Q30.	Are there any additional measures or control that should be considered specifically for cloud resources in the draft RTS, beyond those already identified in Article 37(2)(h) of the proposed draft RTS? If yes, please explain and provide examples.
ICT business continuity management	**Q31.**	Do you agree with the suggested approach regarding ICT business continuity management under the simplified ICT risk management framework? If not, please explain and provide alternative suggestion as necessary.
Report on the ICT risk management framework review	**Q32.**	Do you agree with the suggested approach regarding the article on Format and content of the report on the simplified ICT risk management review? If not, please explain and provide alternative suggestion as necessary.

SESSION 2: RTS to specify the policy on ICT services performed by ICT third-party providers

Francesco Mauro, Head of Unit EBA

Overview of the legal mandate conferred on the ESAs

Article 28(10)
RTS to further specify the detailed content of the policy on the use of ICT services supporting critical or important functions provided by ICT TPPs

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****.*

Article 28 (2)
Strategy on ICT third-party risk

As part of their ICT risk management framework, financial entities, other than entities referred to in Article 16(1), first subparagraph, 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 6(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 basis and, where relevant, on a sub-consolidated and consolidated basis.*** *The management body shall, on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services, regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions.*

The draft RTS in a nutshell

- The draft RTS sets out requirements for **the policy of financial entities on their use of ICT third party service providers, including ICT intra-group TPPs** and concerns all ICT services provided by them that support C&I functions.

- The use of ICT service from ICT TPPs **cannot reduce the responsibility for the financial entities and their management bodies to manage their risks and to comply with legislative requirements**, especially when C&I functions are supported by ICT TPPs. The policy should clearly specify and identify the internal responsibilities for the approval, management, control and documentation of contractual arrangements on the use of ICT services.

- **The structure of this policy should follow all the steps of the life cycle** regarding contractual arrangements, starting with the planning phase of obtaining ICT services, including risk assessments and due diligence processes, covering the ongoing service delivery, monitoring and auditing, and ending with the exit from such arrangements.

- The policy shall apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis.

➢ The public consultation includes 9 questions

➢ Deadline to provide your feedback: **11th September** 2023 via **EU Survey**

Background

Proportionality: *The principle of proportionality is already embedded in the legal text (DORA Article 3) and the application of requirements on ICT third-party risk management by financial entities shall be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations.*

Existing sectorial framework*: The draft RTS has been developed considering already existing specifications provided in Guidelines on outsourcing arrangements published by the ESAs and other relevant specifications provided in the EBA Guidelines on ICT and security risk management.*

Intra-group TPPs*: The draft RTS applies to ICT services provided by ICT intra-group service providers. As per DORA recital (31), intra-group provision of ICT services entails specific risks and benefits however it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework. However, when ICT services are provided from within the same financial group, financial entities might have a higher level of control over intra-group providers, which ought to be taken into account in the overall risk assessment.*

Overview of draft RTS (1/4)

Articles 1-3

The policy shall:

- Take into account **elements of increased complexity or risk** (e.g. location of ICT TPP, nature of data shared, location of data processing and storage, etc.);
- **Implemented consistently across the group subsidiaries**, and adequate for its effective application at all relevant levels;
- **Adopted in writing** and reviewed by the management body **at least once a year** with necessary updates;
- Define or refer to **a methodology for determining which ICT services** support C&I functions;
- Clearly **assign the internal responsibilities** for the approval, management, control, and documentation of relevant contractual arrangements;
- Foresee **assessment of ICT TPP's resources** to ensure compliance with all legal and regulatory requirements;
- Ensure **consistency of relevant contractual arrangements** with the financial entity's ICT risk management framework, information security policy, business continuity policy;
- Require **independent review and inclusion in the financial entity's audit plan**.

Overview of draft RTS (2/4)

Articles 4-6

The policy shall:

- **differentiate**, including for sub-contractors, between the (a) authorised or registered ICT TPPs, including ICT TPPs subject to the oversight framework, (b) ICT intra- group TPPs and TPPs outside the group; (c) ICT TPPs located within the EU and in third countries;
- **specify the requirements for each main phase of the lifecycle** of the use of such ICT services, covering at least (a) responsibilities of the management body, (b) planning, including the risk assessment, due diligence and approval process of new or material changes, (c) involvement of business units, internal controls and others relevant units, (d) implementation, monitoring and management of relevant contractual arrangements, (e) documentation and record-keeping, and (f) the exit strategies and termination processes;
- **define the business** needs before entering into contractual arrangements;
- **require a risk assessment before entering** into a relevant contractual arrangement.

Overview of draft RTS (3/4)

Articles 7-8

The policy shall:

- specify an appropriate and proportionate **process for selecting and assessing the prospective ICT TPP** and prescribe certain aspects the financial entity needs to assess for the ICT TPP, before entering into a contractual arrangement (e.g. business reputation, expertise resources, information security standards, appropriate organisational structure, use of sub-contractors, data location, process, storage, possibility of audits, acting on ethical and socially responsible manner, etc.);
- specify the **required level of assurance concerning the effectiveness of ICT TPPs' risk management framework** and require the assessment of the existence of risk mitigation and business continuity measures;
- determine the **due diligence process** for selecting and assessing the prospective TPPs and consider certain elements in this regard (e.g. audit reports etc.);
- specify the appropriate **measures to identify, prevent and manage actual or potential conflicts of interest** arising from the use of ICT TPPs before entering relevant contractual arrangements and provide for an ongoing monitoring of conflicts of interests.

Overview of draft RTS (4/4)

Articles 9-11

The policy shall:

- specify the requirement for a **written contractual arrangement**, which shall include **information access, inspection, audit, and ICT testing rights**. For this purpose, the financial entity shall use (a) its own internal audit or an appointed third party, (b) pooled audits and pooled ICT testing, including TLPT, (c) third-party certifications and third-party/ internal audit reports made available by the ICT TPP;
- specify whether **third-party certifications and reports are adequate and sufficient** to comply with financial entities' regulatory obligations and **shall not rely solely on these reports over time**. Use of these methods **only under conditions** (e.g. satisfactory audit plan, sufficient coverage of systems and key controls, etc.);
- specify the measures and key indicators **to monitor, on an ongoing basis, the performance of ICT TPPs**, including measures to monitor compliance, and also specify measures when service levels are not met;
- prescribe how the financial entity shall **assess that the ICT TPPs meet appropriate performance and quality standards**. To document the assessment and use its results to update the financial entity's risk assessment;
- define **appropriate measures in case of shortcomings** and monitoring of the implementation of such measures;
- include requirements for a documented *exit plan for each ICT service* and their periodic review and testing.

SESSION 3: RTS on criteria for the classification of ICT-related incidents

Antonio Barzachki, Senior Policy Expert EBA

Background and legal basis

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.

Criteria for classification of major ICT-related incidents (Art. 18(1) DORA):

- 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**;
- the **duration** of the ICT-related incident, including the service downtime;
- the **geographical spread** with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;
- the **data losses** that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;
- the **criticality of the services affected**, including the financial entity's transactions and operations;
- the **economic impact**, in particular costs and losses, of the ICT-related incident in both absolute and relative terms.

Overview of the legal mandate conferred on the ESAs

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**.*

*The ESAs shall take into account the **proportionality** criteria set out in Article 4(2) DORA and **international standards, guidance and specifications** developed and published by ENISA.*

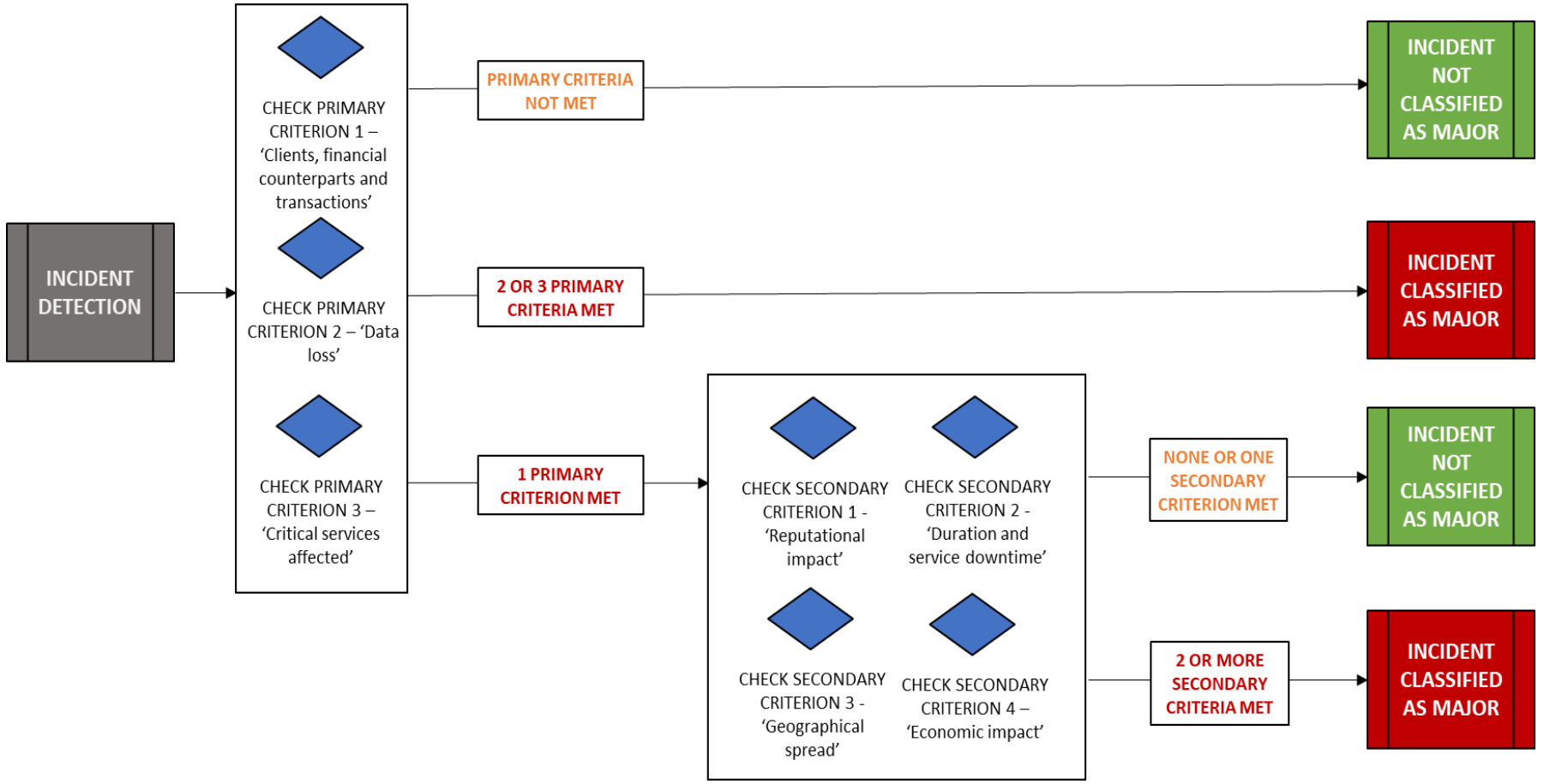
Deadline to deliver – 12 months

Classification of ICT-related incidents – general approach

Approach for classification of major ICT-related incidents (Art. 8)

The CP proposes to classify incidents as major if any of the following conditions are fulfilled:

- the classification thresholds of **two primary criteria** have been met; or
- the classification thresholds of **three or more criteria** have been met, including at least **one primary criterion**.



Classification of ICT-related incidents – criteria & thresholds

Criterion	Specification of the criterion	Materiality threshold
1. Affected clients, financial counterparts, transactions (Art. 1 and 9)		
• Number of affected clients	All affected clients making use of the service. Covering both natural and legal persons.	**10%** of all clients, or **50 000** clients
• Number of affected financial counterparts	All affected financial counterparts having concluded a contractual arrangement with the FE related to the service.	**10%** of all financial counterparts
• Number of affected transactions	Transactions with monetary value.	**15 000 000 EUR**, or **10%** of regular level of transactions,
• Relevant clients or financial counterparts	The impact will affect the business objectives of the FE or market efficiency.	**Any impact** (yes/no)
2. Reputational impact (Art. 2 and 10)	Take into account level of visibility, in particular: - Media attention - Complaints received from different stakeholders - Compliance with regulatory requirements - Loss of clients or financial counterparts	**Any impact** (yes/no)

Classification of ICT-related incidents – criteria & thresholds

Criterion	Specification of the criterion	Materiality threshold
3. Duration and service downtime (Art. 3 and 11)		
• Duration of the incident	Measured from the moment the incident occurs until the moment when it is resolved.	**24 h**
• Service downtime	Measured from the moment the service is unavailable to clients/financial counterparts to the moment when regular activities have been restored.	**2 h** for ICT services supporting critical functions (unless stricter req. stem from DORA or other EU law)
4. Geographical spread (Art. 4 and 12)	Impact in at least two Member States on: - clients or financial counterparts; or - branches of the financial entity; or - FEs within the group; or - financial market infrastructures; or - third-party providers common with other FEs.	**Any impact** (yes/no)
5. Data losses (Art. 5 and 13)	Clarification of the data losses that the incident entails in relation to the availability, authenticity, integrity and/or confidentiality of data.	**Any significant impact** (yes/no) on **critical data** (impact on business objectives and compliance)

Classification of ICT-related incidents – criteria & thresholds

Criterion	Specification of the criterion	Materiality threshold
6. Critical services affected (Art. 6 and 14)	Impact on the activities that require authorisation, or ICT services that support critical or important functions.	**Any impact** (yes/no) and **escalation** to senior management or management body
7. Economic impact (Art. 7 and 15)	The following types of direct or indirect costs and losses to be taken into account • expropriated funds or financial assets for which the financial entity is liable, including assets lost to theft; • replacement or relocation costs of software, hardware or infrastructure; • staff costs; • fees due to non-compliance with contractual obligations; • customer redress and compensation costs; • losses due to forgone revenues; • costs associated with internal and external communication; • advisory costs. FEs shall not take into account costs for running the business as usual.	Gross costs and losses higher than **100 000 EUR**

Recurring incidents, significant cyber threats, relevance to other jurisdictions and information to be shared

Recurring incidents (Art. 16)

- **Recurring incidents** that individually do not constitute a major incident shall be considered as **one major incident** where the incidents, in aggregate and over a **period of the preceding 3 months**, meet the classification criteria and thresholds.
- The recurring incidents shall **occur at least twice**, have the same apparent **root cause** and shall be with similar **nature and impact**.

Criteria and thresholds for determining significant cyber threats (Art. 17)

Conditions to be met for cyber incidents to be considered significant:

- the cyber threat could **affect critical or important functions** of the financial entity, other financial entities, third party providers, clients or financial counterparts;
- the cyber threat has a **high probability of materialisation** (risks, capabilities and intent of threat actors, persistence of the threat and any accrued knowledge) at the financial entity or other financial entities; and
- the cyber threat could **fulfil the conditions for major ICT-related incidents** if it materialises.

Relevance to competent authorities in other Member States (Art. 18) – same approach as 'geographical spread criterion'.

Details of major incidents to be reported to other authorities (Art. 19) – all data reported to the CA, without any anonymization.

Overview of the questions asked

Question 1. Do you agree with the overall approach for classification of major incidents under DORA? If not, please provide your reasoning and alternative approach(es) you would suggest.

Questions 2-5. Do you agree with the specification and materiality thresholds of the classification criteria as proposed in Articles 1-7 and 9-15 of the draft RTS? If not, please provide your reasoning and suggested changes.

Question 6. Do you agree with capturing recurring incidents with same apparent root cause, similar nature and impact, that in aggregate meet the classification criteria and thresholds as major incidents under DORA, as proposed in Article 16? If not, please provide your reasoning and suggested changes. Please also indicate how often you face recurring incidents, which in aggregate meet the materiality thresholds only over a period of 6 to 12 months based on data from the previous two years (you may also indicate the number of these recurring incidents).

Question 7. Do you agree with the approach for classification of significant cyber threats as proposed in Articles 17? If not, please provide your reasoning and suggested changes.

Question 8. Do you agree with the approach for assessment of relevance of the major incidents in other Member States and the level of details to be shared with other authorities, as proposed in Articles 18 and 19? If not, please provide your reasoning and suggested changes.

SESSION 4: ITS to establish the templates for the register of information

Andrea Vetrone, Senior Expert on Supervisory Oversight EIOPA

Overview of the legal mandate conferred on the ESAs

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.

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)*

The draft ITS and the Register of Information in a nutshell

- The **draft ITS is technology agnostic and does not cover the process of sharing information** from FEs to CAs and from the CAs to the Oversight Forum. However, templates and requirements have been designed a data management (**relational structure**) and reporting perspective to ensure **consistency and harmonisation by design**.
- Almost each template is a table with a predefined number of columns but an indefinite number of rows (**open table**).
- **Templates are proportionate by design**, since the quantity of information to be included depends on the extent of FE's dependency on services provided by ICT TPPs. Additional information to be reported only if the ICT service supports critical or important functions.
- **Design** of the templates **leverage on the lessons learned** of ESAs and CAs data collection on outsourcing and third-party arrangements.
- The **templates** included in the draft ITS **aim to identify**:

  a) minimum and necessary information on **contractual arrangements** and on **risk assessment and due diligence** performed by FEs

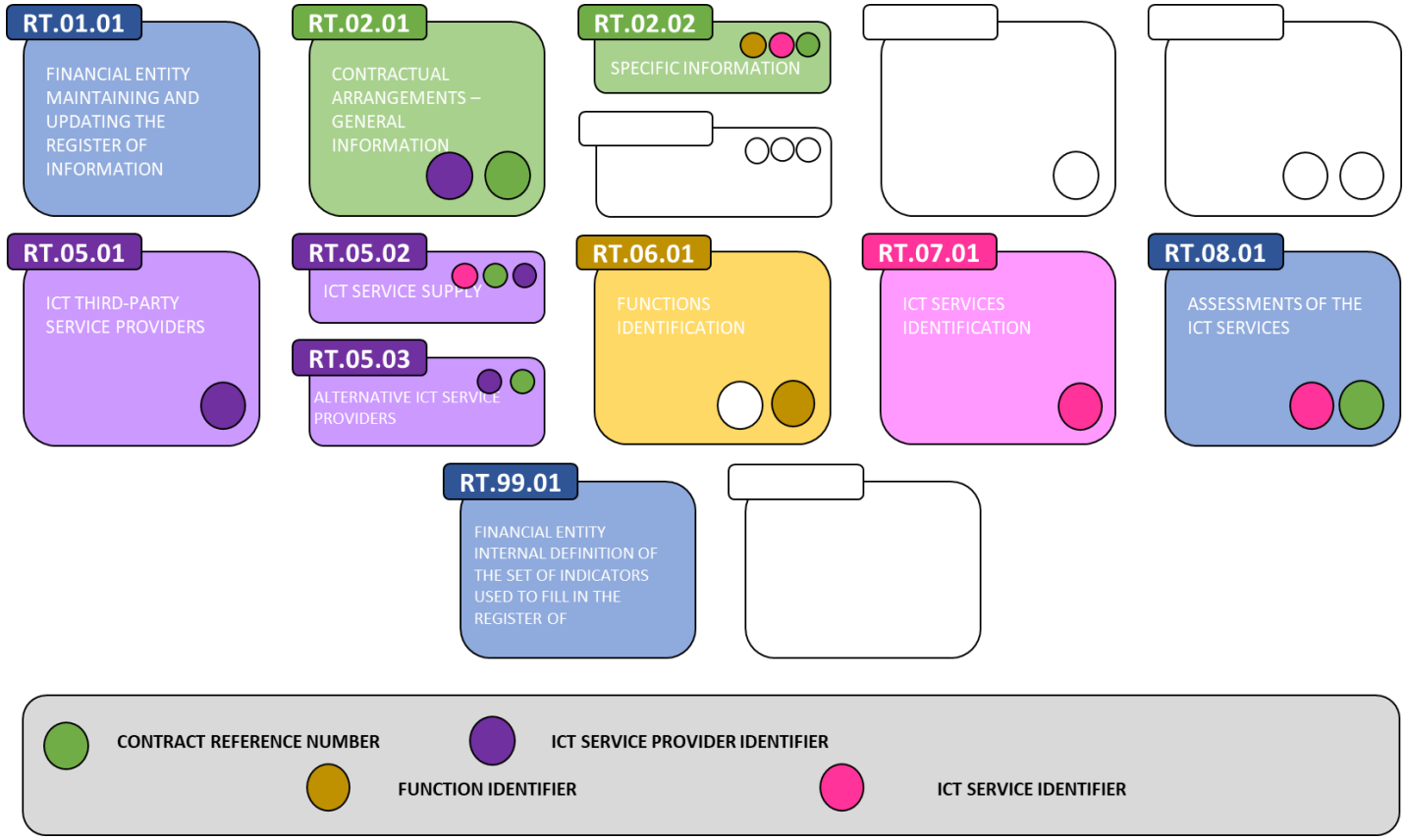
  b) the **link between functions** of the FEs **and ICT services** provided by ICT TPPs

  c) the **ICT service supply chain** with a focus on material subcontractors

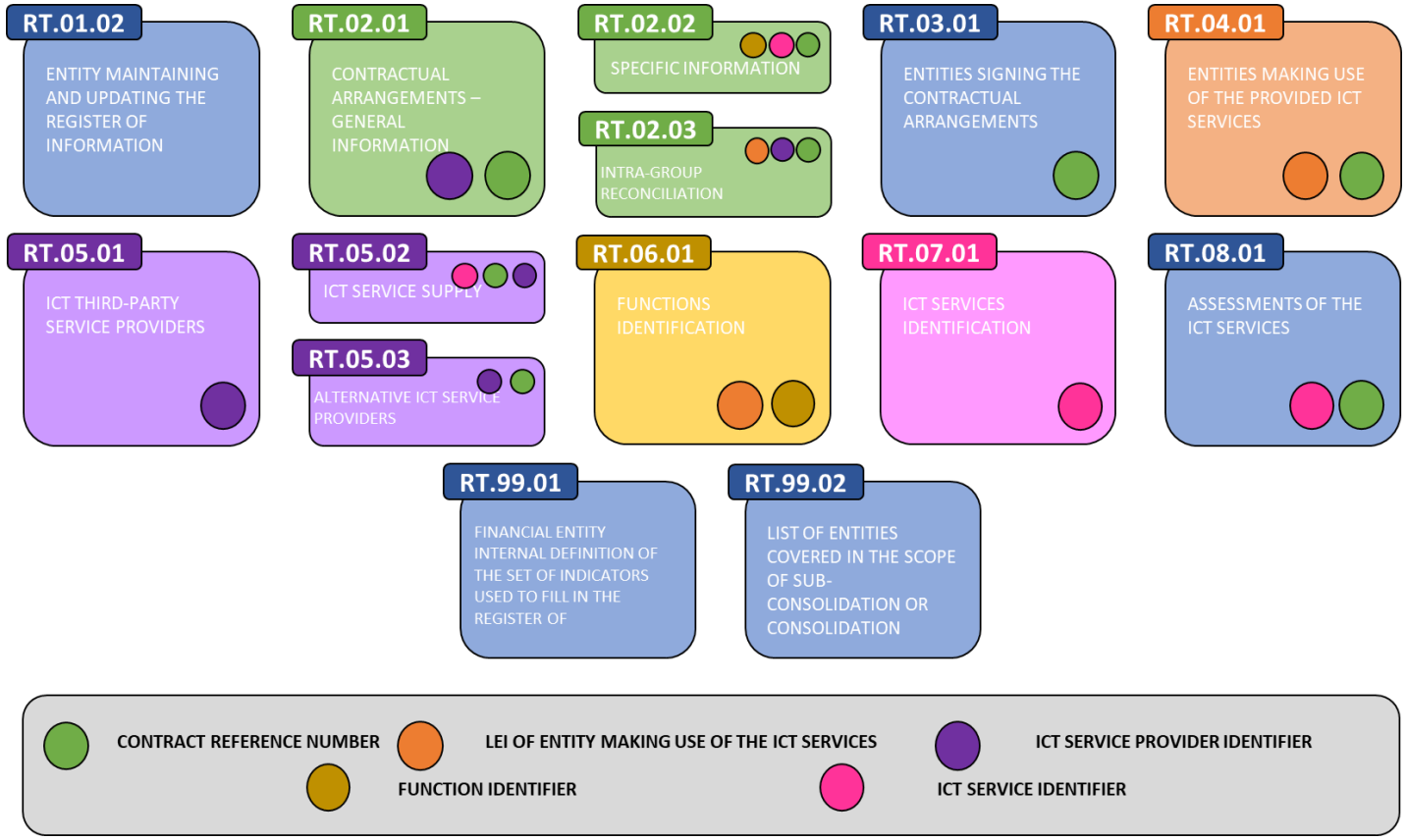
  d) unambiguously and consistently the **ICT TPPs** (incl. subcontractors) **and the FEs by** using a Legal Entity Identifier (**LEI**) code

- Each FE shall maintain and update a register of information at (i) entity level; (ii) sub-consolidated level and consolidated level. The **scope of (sub)consolidation is defined by the ultimate parent undertaking** taking into account the applicable financial regulations.

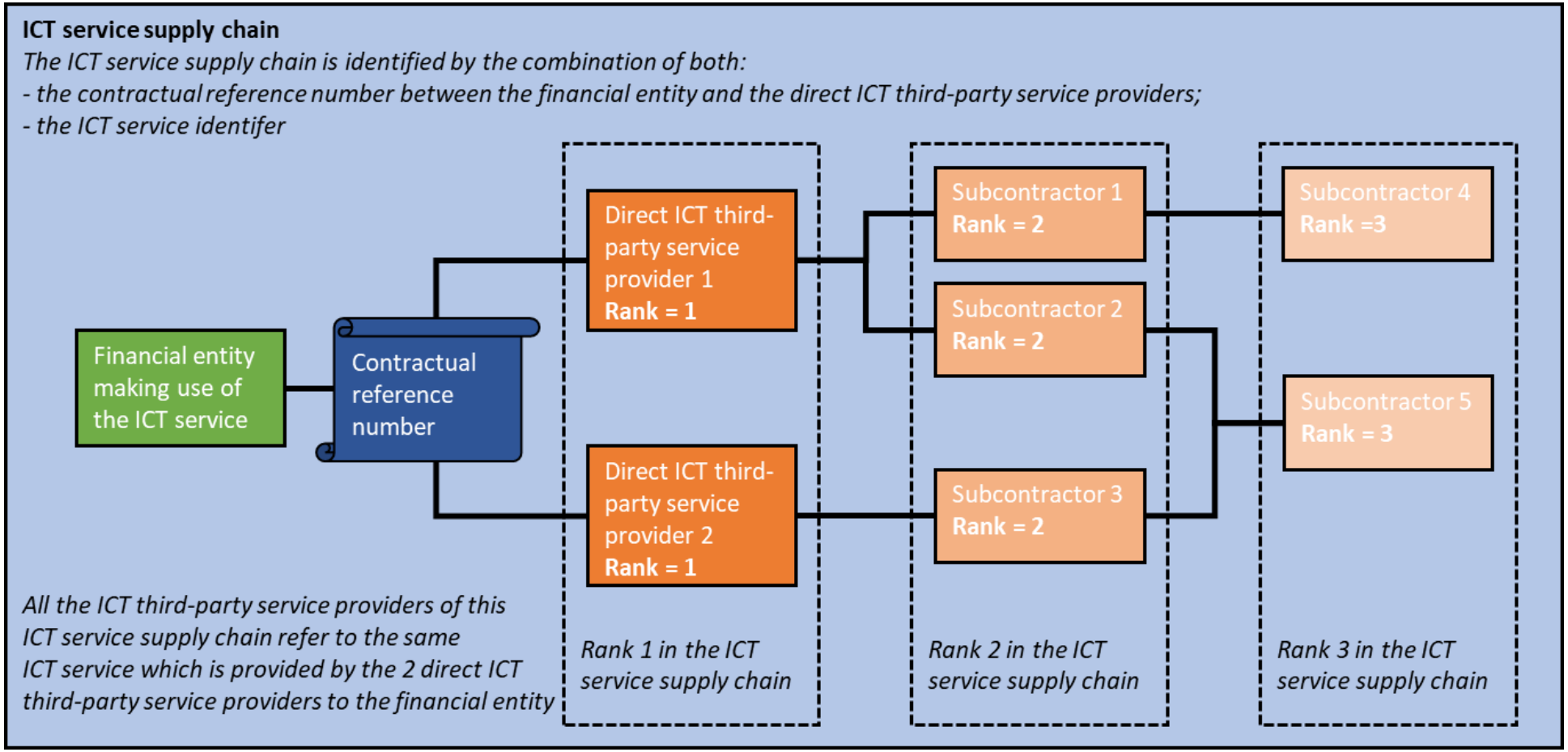
Structure of the templates (entity level)



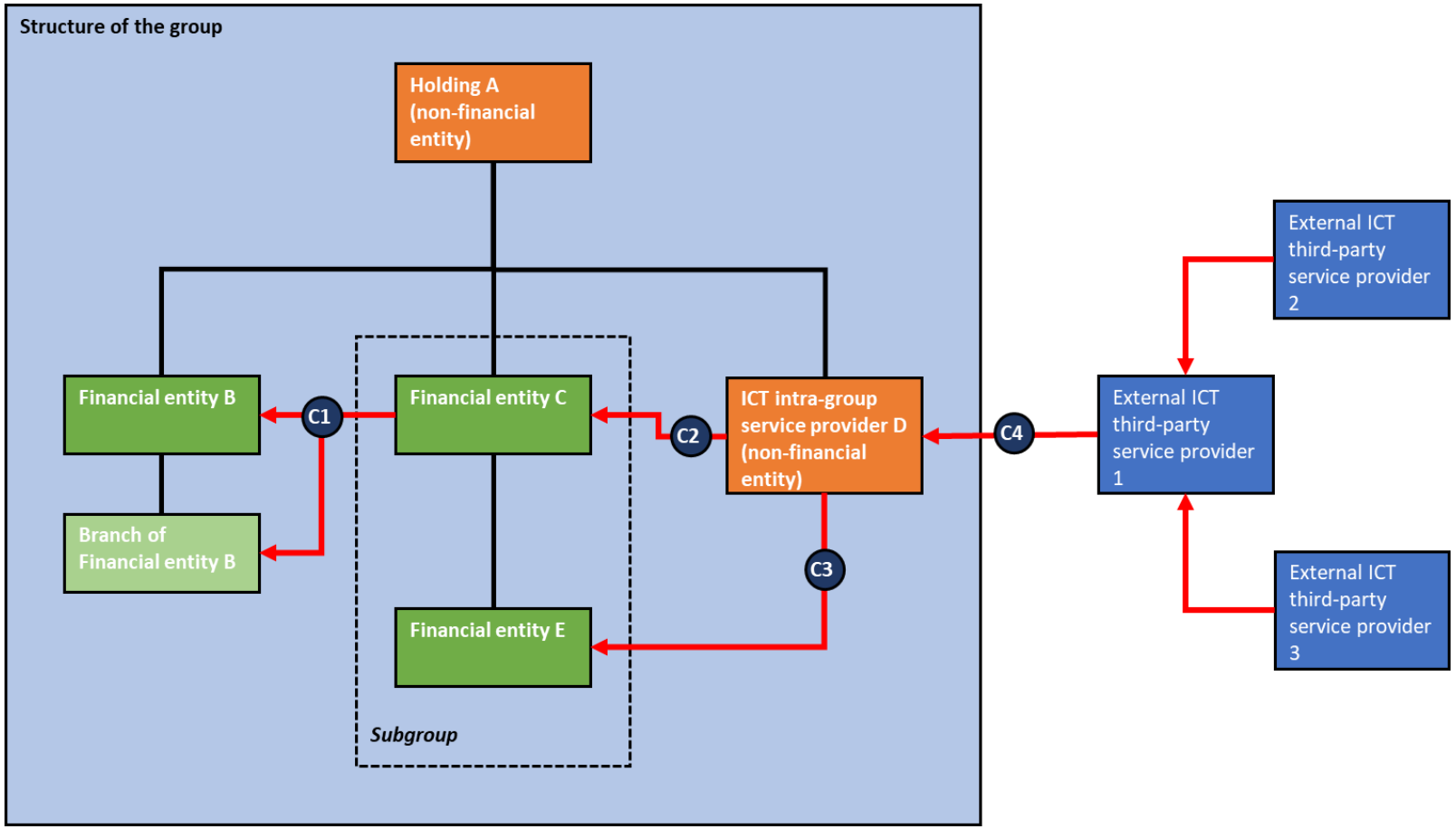
Structure of the templates (sub-consolidated and consolidated level)



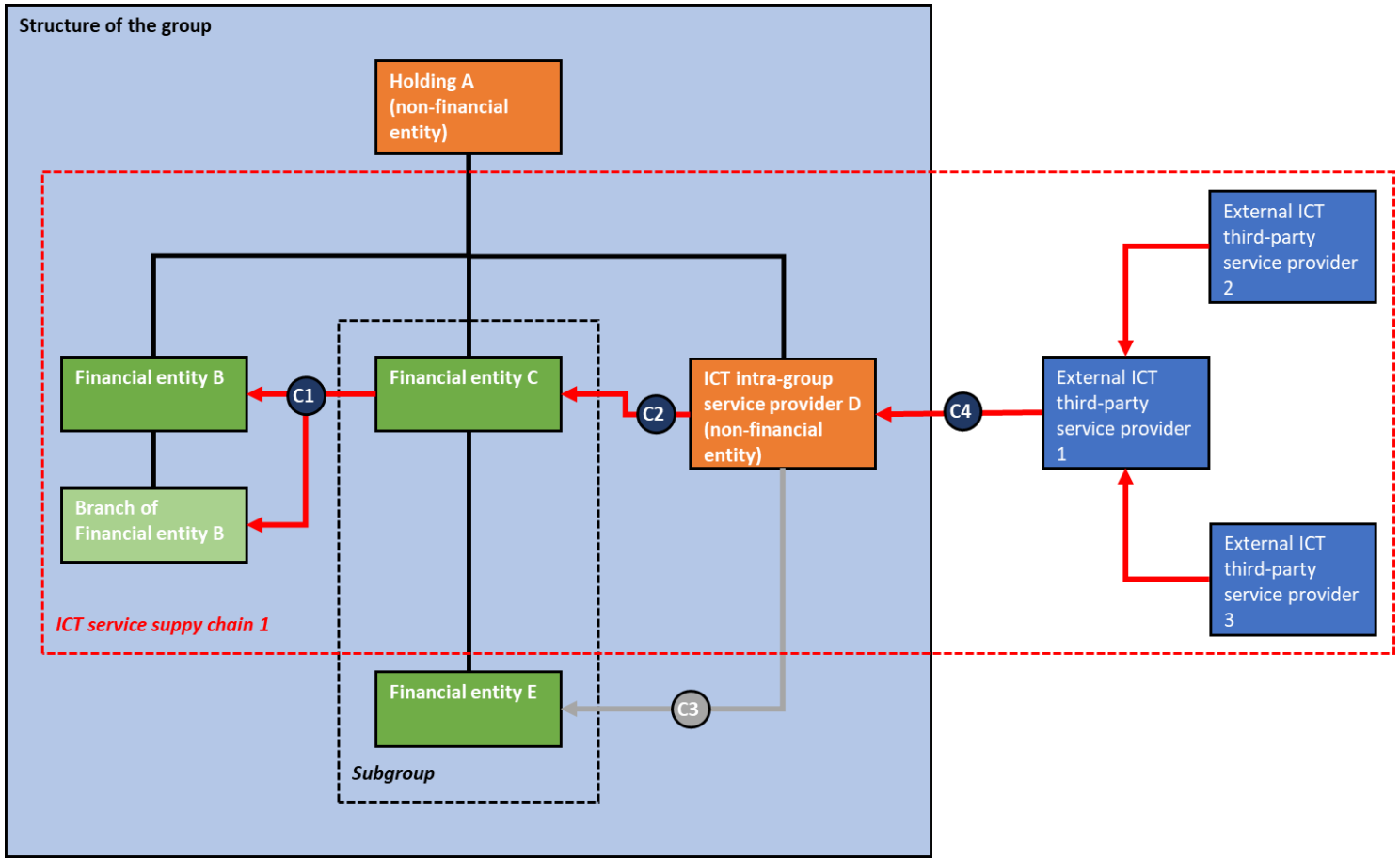
ICT service supply chain in a nutshell



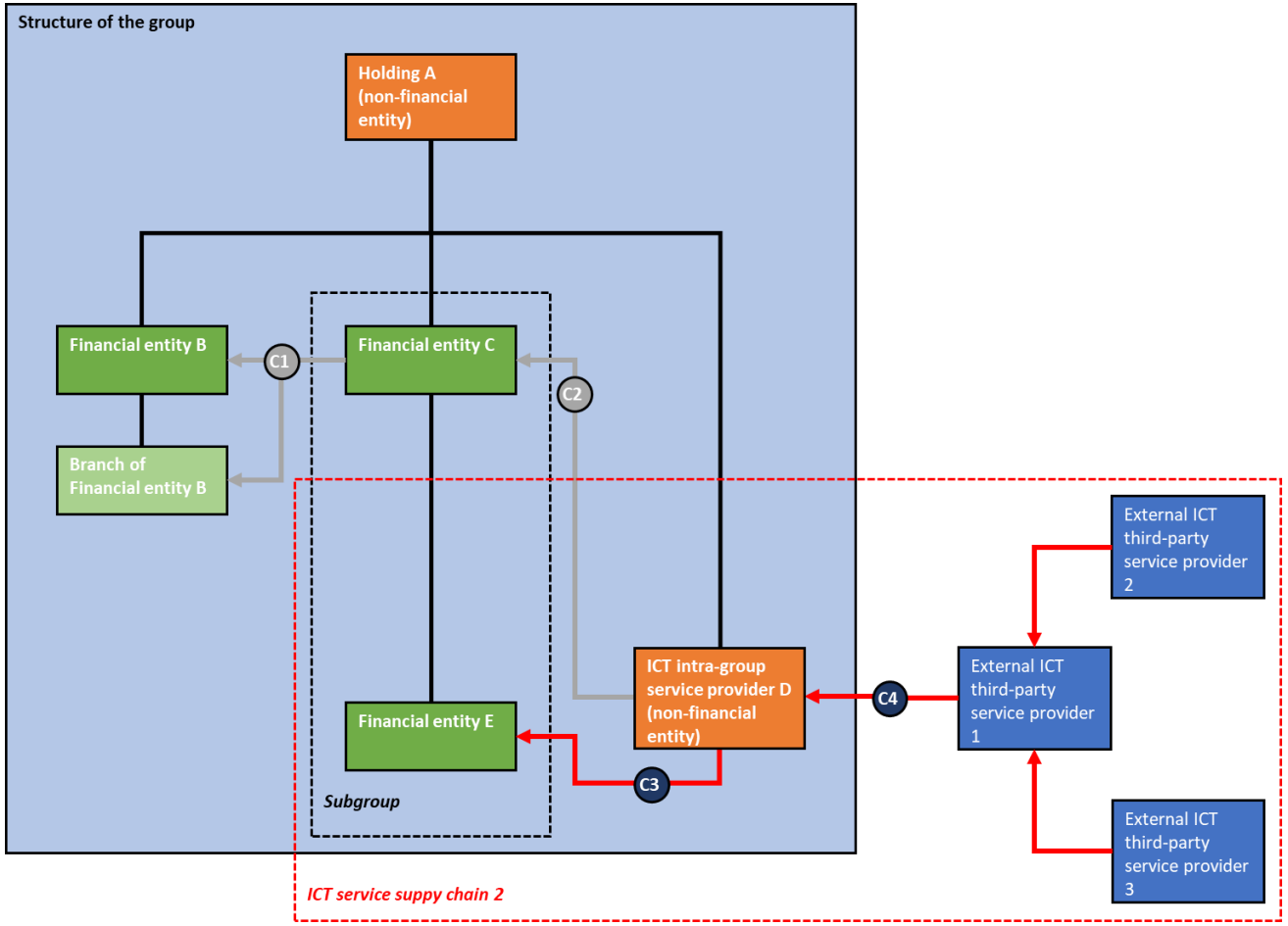
Example: ICT service supply chain



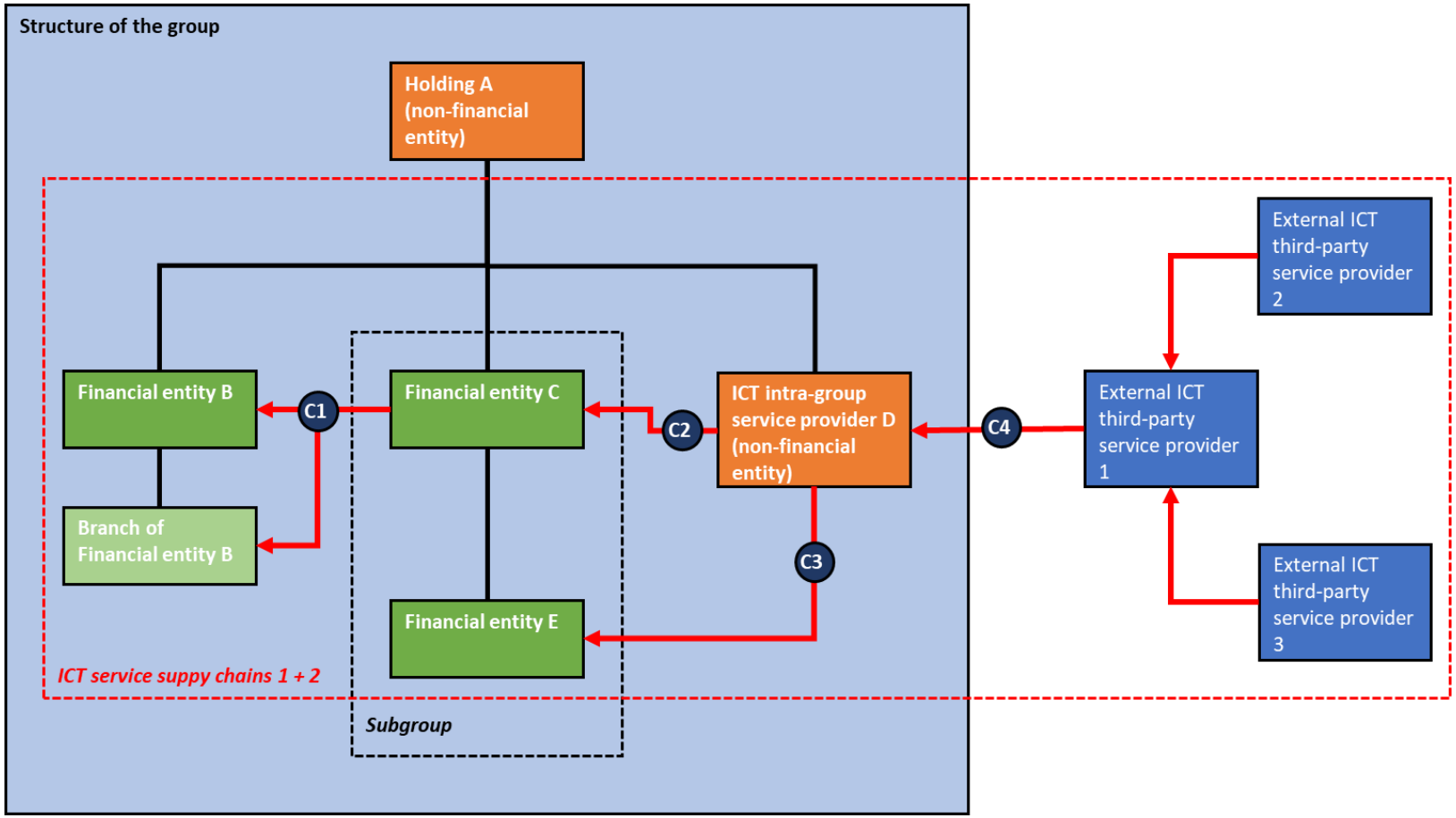
Example: ICT service supply chain 1 – from financial entity B perspective



Example: ICT service supply chain 2 – from financial entity E perspective



Example: ICT service supply chains 1 + 2 – from consolidated perspective



Overview of the consultation questions

- The consultation paper (CP) includes 14 questions covering the following areas:
  - Use of the LEI code;
  - Inclusion of all material sub-contractors in the scope of the register of information, considering Article 28(3) of DORA;
  - First implementation of the register of information;
  - Requirement to keep information on terminated arrangements for 5 years;
  - Register of information at (sub)consolidated level;
  - Inclusion of information on the annual expenses / budget of the contractual arrangement;
  - ICT service supply chain;
  - Taxonomy of ICT services;
  - Instructions to report the total value of assets and the value of other financial indicator;
  - The overall structure of, the level of information requested in, and the principle used to draft the register of information;
  - The conclusions of the impact assessment.
- The CP invites also the stakeholders to provide feedback on each of the columns of each templates via dedicated Excel file (downloadable from and to be uploaded after in the EU Survey)

Next steps

	DORA policy work	Article	Public consultation	Finalise
	Call for advice on criticality criteria and fees	31.8 | 43.2	26 May - 23 June 23	30 Sept 2023
FIRST BATCH	RTS on ICT risk management framework	15		
	RTS on simplified ICT risk management framework	16		
	RTS on criteria for the classification of ICT-related incidents	18.3	19 June - 11 Sept 23	17 Jan 2024
	ITS to establish the templates for the Register of information	28.9		
	RTS to specify the policy on ICT services performed by 3rd party	28.1		
SECOND BATCH	RTS on specifying the reporting of major ICT-related incidents	20.a		
	ITS to establish the reporting details for major ICT-related incidents	20.b		
	Guidelines on the estimation of aggregated costs/losses caused by major ICTrelated incidents	11.11		
	RTS to specify threat led penetration testing aspects	26.11	Nov/Dec 23 - TBC	17 June 2024
	RTS to specify elements when sub-contracting critical or important functions	30.5		
	GL on cooperation between ESAs and CAs regarding the structure of the oversight	32.7		
	RTS to specify information on oversight conduct	41		
	Feasibility report on single EU Hub for major ICT-related events	21	TBC	17 January 2025

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.
  - ESMA's Questions and Answers (europa.eu)
  - EBA's Questions and Answers (europa.eu)
  - EIOPA's Questions and Answers (europa.eu)