REPLY

EU DORA Reforms

Overview of the Joint Consultation on the First Batch of DORA Policy Products

7th July 2023

FSQS REGISTERED

UK FINANCE 2023 ASSOCIATE MEMBER

Contents

Section 1: Introduction

Section 2A: Regulatory Technical Standards (RTS) on ICT Risk Management Framework and Simplified ICT Risk Management Framework

Section 2B: RTS on Criteria for the Classification of ICT-related Incidents

Section 2C: RTS to Specify the Policy on ICT Services Performed by ICT Third-Party Providers

Section 2D: Implementing Technical Standards (ITS) to establish the Templates for the Register of Information

Section 3: Next Steps

Appendix

Section 1: Introduction

Introduction (1/2)

The Digital Operational Resilience Act (DORA)

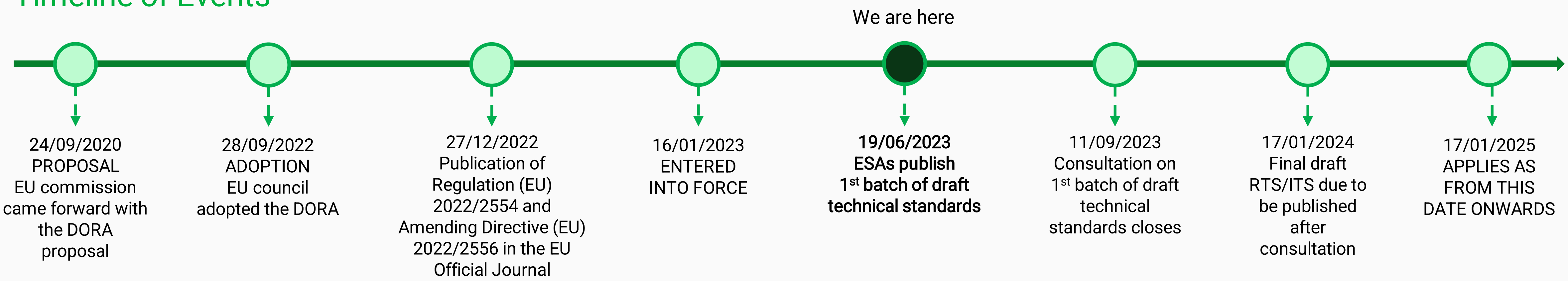
On 19th June 2023 The European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) launched a public consultation on the first batch of policy products under the DORA.

This pack provides an overview of the four draft regulatory technical standards (RTS) and one set of draft implementing technical standards (ITS) released.

The DORA proposal is part of a larger EU digital finance package, which aims to develop an EU-wide approach that fosters technological development and ensures financial stability and consumer protection.

The DORA sets uniform requirements for the security of network and information systems of financial services firms as well as Critical Third Parties (CTPs) which provide ICT (Information Communication Technologies) related services to them. DORA creates a regulatory framework whereby firms need to make sure they can withstand, respond to, and recover from ICT-related disruptions and threats.

Timeline of Events



We are here

24/09/2020
PROPOSAL
EU commission came forward with the DORA proposal

28/09/2022
ADOPTION
EU council adopted the DORA

27/12/2022
Publication of Regulation (EU) 2022/2554 and Amending Directive (EU) 2022/2556 in the EU Official Journal

16/01/2023
ENTERED INTO FORCE

19/06/2023
ESAs publish 1st batch of draft technical standards

11/09/2023
Consultation on 1st batch of draft technical standards closes

17/01/2024
Final draft RTS/ITS due to be published after consultation

17/01/2025
APPLIES AS FROM THIS DATE ONWARDS

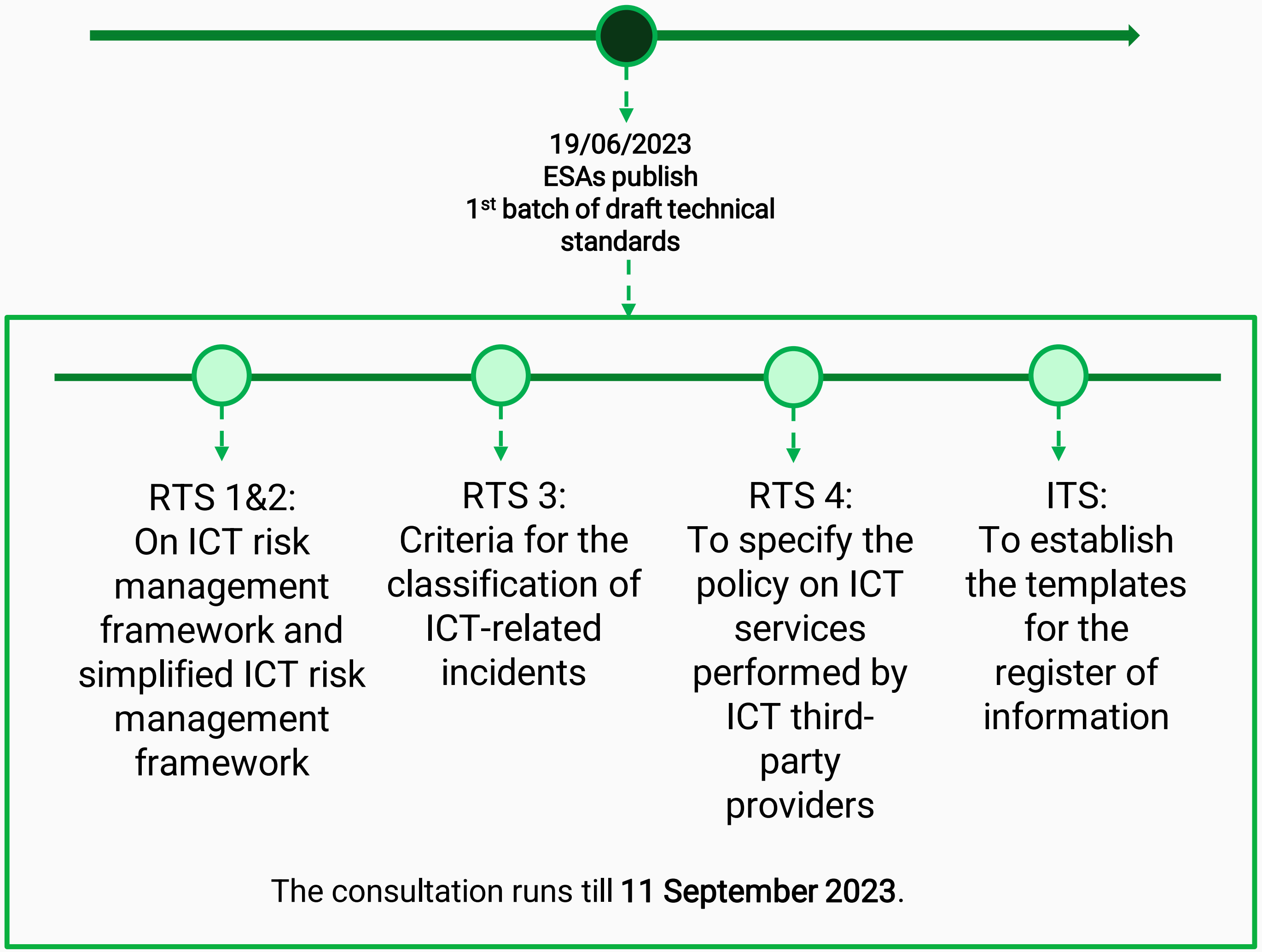
Source: Joint Consultation on the First Batch of DORA Policy Products

Introduction (2/2)

DORA mandates the ESAs to prepare through the Joint Committee (JC), a set of policy products with two main submission deadlines: 17 January 2024 (first batch) and 17 June 2024 (second batch).

The first batch consists of four draft RTS and one set of draft ITS. Based on the feedback received to the public consultation, the legal instruments will be finalised and will be submitted to the European Commission by 17 January 2024.

These technical standards aim to ensure a consistent and harmonised legal framework in the areas of ICT risk management, major ICT-related incident reporting and ICT third-party risk management.



19/06/2023
ESAs publish
1st batch of draft technical standards

RTS 1&2:
On ICT risk management framework and simplified ICT risk management framework

RTS 3:
Criteria for the classification of ICT-related incidents

RTS 4:
To specify the policy on ICT services performed by ICT third-party providers

ITS:
To establish the templates for the register of information

The consultation runs till **11 September 2023**.

Section 2A: Draft RTS 1 & 2

To further harmonise ICT risk management tools, methods, processes and policies

Overview of Draft RTS 1 & 2 – ICT Risk Management

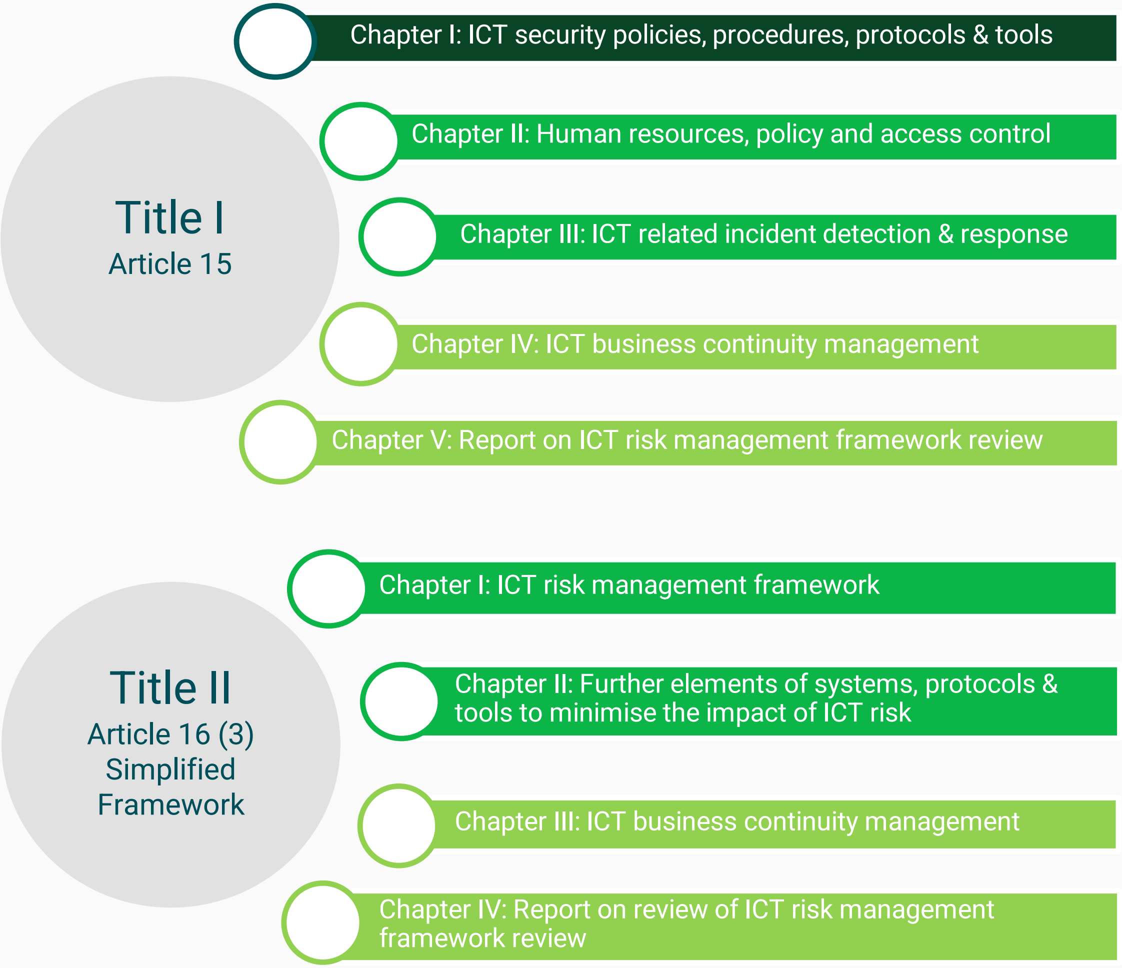
PURPOSE: To provide more specific guidance to financial entities (FEs) on the requirements for ICT risk management, with a simplified framework provided under Title II for the small and non-interconnected firm.

KEY MESSAGES:

- To ensure coherence between the provisions for FEs in scope of DORA, the consultation paper (CP) combines the two RTS relating to the ICT risk management framework into a single RTS divided into two titles.
- The first aims to provide further harmonisation of existing ICT risk management tools, methods, processes and policies. The second specifies the requirements that should apply to small and non-interconnected firms.

Principles of the CP

1. **Technology Neutral** – The ESAs have tried to 'future-proof' the Consultation Paper (CP) by intentionally avoiding reference to specific technologies and products.
2. **Cross Sectoral** – Due to the wide range of entities that fall within the scope of DORA, requirements outlined are generally principle based and sector agnostic so as to be applicable to all relevant entities where possible.
3. **Proportionality** – is taken into consideration throughout the CP, and primarily embedded within the CP through the delineation between Titles I and II, and the FEs they apply to.



Title I
Article 15

Chapter I: ICT security policies, procedures, protocols & tools

Chapter II: Human resources, policy and access control

Chapter III: ICT related incident detection & response

Chapter IV: ICT business continuity management

Chapter V: Report on ICT risk management framework review

Title II
Article 16 (3)
Simplified
Framework

Chapter I: ICT risk management framework

Chapter II: Further elements of systems, protocols & tools to minimise the impact of ICT risk

Chapter III: ICT business continuity management

Chapter IV: Report on review of ICT risk management framework review

Section 2B: Draft RTS 3

Specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats

Overview of Draft RTS 3 – Defining Major Incidents and Classification Criteria

PURPOSE: this CP outlines:

- The classification criteria for ICT-related incidents or, as applicable, operational or security payment-related incidents
- Materiality thresholds for determining major incidents
- The criteria and materiality thresholds for determining significant cyber threats
- Criteria for competent authorities (CAs) to assess relevance of incidents to CAs in other Member States and details of the incidents to be shared with other CAs

KEY MESSAGES

The CP provides a definition of Major Incidents.

The ESA's propose 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 (primary and secondary) specified have been met, including at least one primary criterion

Primary Criteria

1: Clients, financial counterparts and transactions affected
This captures all clients, which may be natural or legal persons, that have been affected by the incident. The materiality threshold covers relative and absolute numbers of clients and value of transactions.

2: Data Losses
The CP proposes a qualitative binary threshold (yes/no answer), with the FE indicating whether the incident has entailed any loss of critical data related to availability, authenticity, integrity or confidentiality.

3. Critical Services Affected
This should allow for the capture of specific cases where the incident has impacted (i) the provision of financial services that require authorization/registration in the EU or (ii) ICT services that support critical or important functions of the FE.
It will have to also be dependent on whether the incident has been escalated to the senior management, such that escalation is distinguished from regular reporting.

Secondary Criteria

4. Reputational Impact
The threshold proposed is qualitative and binary (yes/no answer). The draft RTS specifies how reputational impact can materialize, e.g. attraction of media attention, complaints received from clients, incompliance with regulatory requirements as a result of the incident or whether the FE has lost or is likely to lose clients.

5. Duration and Service Downtime
The duration of an incident needs to be measured from the moment the incident occurs until the moment when the incident has been resolved. the threshold for service downtime should be consistent with existing incident reporting frameworks.

6. Geographical Spread
The criterion is based on the FE's own assessment of the material impact in two or more jurisdiction(s).

7. Economic Impact
ESAs propose to use a single absolute number of EUR 100 000 or above for the gross direct and indirect costs and losses incurred by the incident, with a non exhaustive list of direct and indirect costs and losses to include (and not to include) provided in the RTS.

Section 2C: Draft RTS 4

To specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers

Overview of Draft RTS 4 - Policy on ICT Services Performed by ICT TPPs

PURPOSE: This CP further specifies what the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions should include, and the governance surrounding the policy

KEY MESSAGES:

- FEs must define crucial parts of their governance arrangements, risk management and internal control framework with regard to the use of ICT services provided by ICT third-party service providers. **This also includes those ICT service providers for functions that are not classified as critical or important.**
- The draft RTS deals with ICT third party services providers and ICT intragroup service providers in the same way.
- FEs should clearly assign the internal responsibilities for the approval, management, control, and documentation of contractual arrangements applicable to all the phases of the use of such ICT services.
- FEs should define clear assessment criteria and appropriate measures to respond to any shortcomings are clearly identified as part of their due diligence process.

The draft RTS take into consideration existing guidelines on outsourcing and definitions:

ICT Services

Digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

Critical and Important Functions

A function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.

Section 2D: Draft ITS

To establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

Overview of Draft ITS

PURPOSE: The CP includes a set of templates which form the register of information (at entity, sub-consolidated and consolidated levels) in relation to all contractual arrangements on the use of ICT services provided by ICT Third Party Service Providers (ICT TPPs).

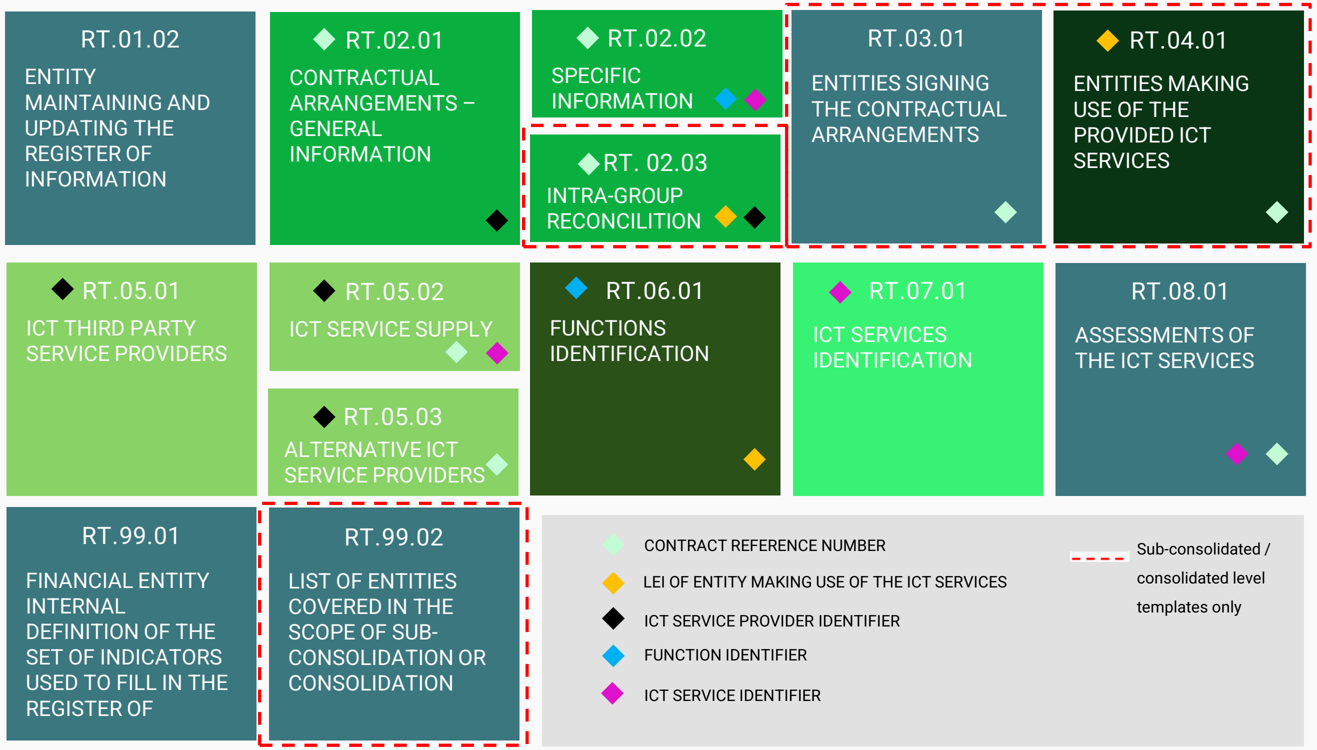
KEY MESSAGES:

- There are **10 templates used by financial entities at entity level. An additional 4 templates (highlighted) are to be used at sub-consolidated and consolidated level** to link the registers of information of the various entities in scope of the group and to ensure there is no double counting.
- The templates are linked to each other by using different specific keys in order to form a relational structure.
- FEs must identify ICT services provided by ICT third-party service providers supporting **all functions**, (not only critical / important)
- In the case of groups, there is the additional need to capture the following links:

  1. contracts between entities within the group only (internal contracts)

  2. contracts between an entity within the group and an external ICT third-party service provider (external contracts)

Structure of the Register of Information



RT.01.02 ENTITY MAINTAINING AND UPDATING THE REGISTER OF INFORMATION

◆ RT.02.01 CONTRACTUAL ARRANGEMENTS – GENERAL INFORMATION ◆

◆ RT.02.02 SPECIFIC INFORMATION ◆ ◆

◆ RT. 02.03 INTRA-GROUP RECONCILITION ◆ ◆

RT.03.01 ENTITIES SIGNING THE CONTRACTUAL ARRANGEMENTS ◆

◆ RT.04.01 ENTITIES MAKING USE OF THE PROVIDED ICT SERVICES ◆

◆ RT.05.01 ICT THIRD PARTY SERVICE PROVIDERS

◆ RT.05.02 ICT SERVICE SUPPLY ◆ ◆

◆ RT.05.03 ALTERNATIVE ICT SERVICE PROVIDERS ◆

◆ RT.06.01 FUNCTIONS IDENTIFICATION ◆

◆ RT.07.01 ICT SERVICES IDENTIFICATION

RT.08.01 ASSESSMENTS OF THE ICT SERVICES ◆ ◆

RT.99.01 FINANCIAL ENTITY INTERNAL DEFINITION OF THE SET OF INDICATORS USED TO FILL IN THE REGISTER OF

RT.99.02 LIST OF ENTITIES COVERED IN THE SCOPE OF SUB-CONSOLIDATION OR CONSOLIDATION

◆ CONTRACT REFERENCE NUMBER

◆ LEI OF ENTITY MAKING USE OF THE ICT SERVICES

◆ ICT SERVICE PROVIDER IDENTIFIER

◆ FUNCTION IDENTIFIER

◆ ICT SERVICE IDENTIFIER

- - - - Sub-consolidated / consolidated level templates only

Next Steps

Next Steps

The ESAs deadline for the submission of comments in response to the consultation is **11 September 2023**.

A public hearing has been organised in the form of a webinar on 13 July 2023 from 09:00 to 18:00 CET. The ESAs have invited interested stakeholders to register using this Registration form by 16:00 CET on 10 July 2023.

Avantage Reply are developing our own response to consultation. If you would like to discuss your own response with us, please feel free to reach out to us - r.abela@reply.com

Contact Us

Vishwas Khanna
Partner
vi.khanna@reply.com

Vishwas has international FS consulting and risk management experience across Europe, the US, the Middle East and SE Asia, leading a multitude of risk transformations and change programmes.

Vishwas is a trusted advisor to the C-Suite and senior management across a number of financial institutions with strong working relationships with industry associations, and academia and is a speaker at industry events and forums. He is also a member of the Institute of Directors, London.

Previously at Deloitte, he led complex risk transformations, Brexit programmes, prudential regulation (ICAAPs, stress testing and risk appetite) and regulatory reporting projects with significant banks (PRA and SSM) and other financial services firms.

Ritianne Abela
Manager
r.abela@reply.com

Ritianne is a highly experienced professional in the financial services industry, with a career spanning over fifteen years. Having worked with two ECB SSM banks, as well as working with one of the industry's top ten international advisory firms.

Throughout her career, Ritianne has held the pen to a number of risk and regulatory documents, such as Risk Management Frameworks, Corporate Governance Frameworks, and Outsourcing Frameworks. Ritianne is used to collaborating with executive leadership, regulators, and supervisory inspectors, consistently demonstrating her ability to navigate complex stakeholder environments. She has successfully implementing numerous remedial action plans.

Her professional portfolio includes corporate governance, enterprise risk management, outsourcing risk, ESG, regulatory affairs, supervisory dialogue, and credit risk.

Adam Wilson
Senior Consultant
ad.wilson@reply.com

Adam has experience with the implementation of financial regulation, working as a UK regulator for over five years. Through his experience as a financial regulator and as a consultant, he has worked with a range of financial firms and has extensive experience interacting with regulatory bodies in Europe and the US, including the ECB, CFTC, and SEC.

He has a deep understanding of regulatory and prudential risk requirements, having conducted a number of specialist reviews relating to both financial and non-financial risks. Adam has regulatory and consulting experience across: the implementation of the PRA Operational Resilience policy, Third Party Risk Management; Liquidity and Capital SREP reviews; CCPs and default management procedures; Governance; Risk Management; and Regulatory Compliance.

Jake Palmer
Senior Consultant
ja.palmer@reply.com

Jake has 5 years' experience working at the Prudential Regulation Authority, supervising a range of UK based financial firms.

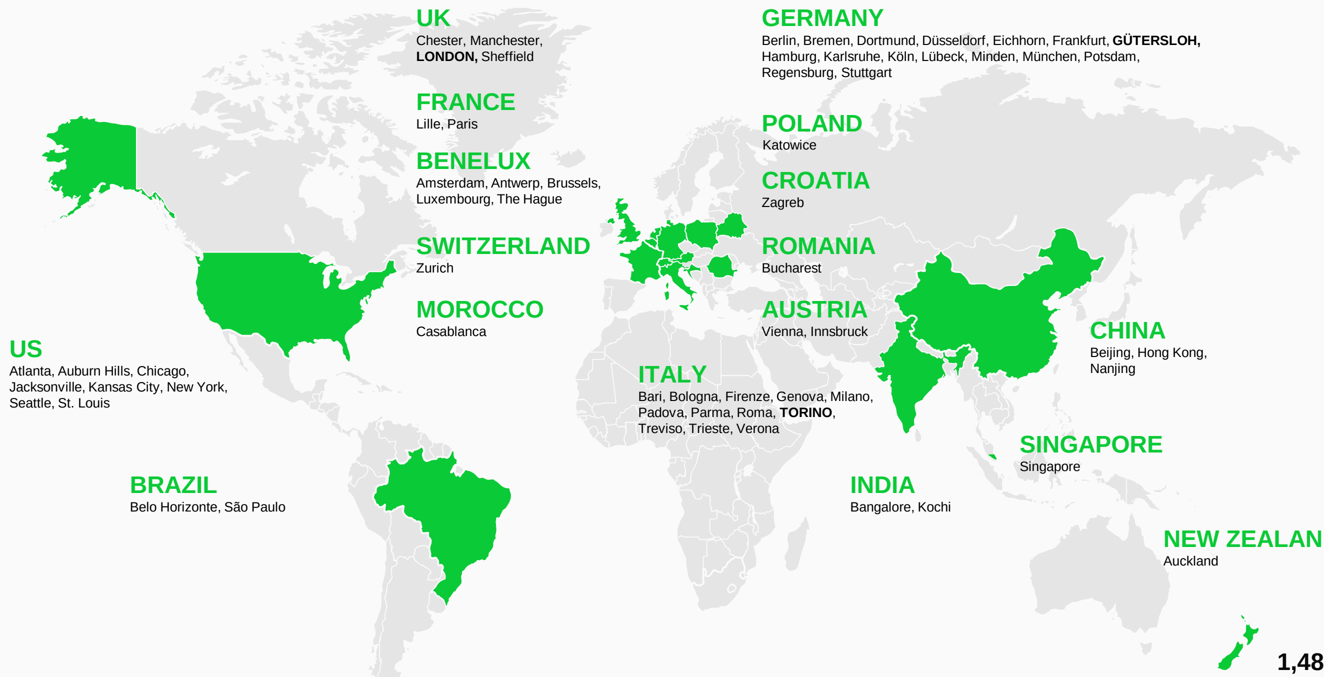
As a result, he has a deep knowledge of bank business models and regulatory issues, and extensive experience in stakeholder management having engaged extensively with firms' executive leadership and other regulatory bodies.

He has worked on a number of prudential risk reviews covering a range of financial and non-financial risks, with regulatory experience across; Capital Supervisory Review and Evaluation Process (SREP) reviews; Operational Resilience, Governance; Risk Management; and Regulatory Compliance.

About Reply

We combine geographical footprint with deep specialist domain expertise

Reply Group – a leading global consulting services partner operating across a number of different segments, combining specific sector expertise with wide experience in delivery services and technology capabilities



UK
Chester, Manchester, **LONDON,** Sheffield

FRANCE
Lille, Paris

BENELUX
Amsterdam, Antwerp, Brussels, Luxembourg, The Hague

SWITZERLAND
Zurich

MOROCCO
Casablanca

US
Atlanta, Auburn Hills, Chicago, Jacksonville, Kansas City, New York, Seattle, St. Louis

BRAZIL
Belo Horizonte, São Paulo

GERMANY
Berlin, Bremen, Dortmund, Düsseldorf, Eichhorn, Frankfurt, **GÜTERSLOH,** Hamburg, Karlsruhe, Köln, Lübeck, Minden, München, Potsdam, Regensburg, Stuttgart

POLAND
Katowice

CROATIA
Zagreb

ROMANIA
Bucharest

AUSTRIA
Vienna, Innsbruck

ITALY
Bari, Bologna, Firenze, Genova, Milano, Padova, Parma, Roma, **TORINO**, Treviso, Trieste, Verona

INDIA
Bangalore, Kochi

CHINA
Beijing, Hong Kong, Nanjing

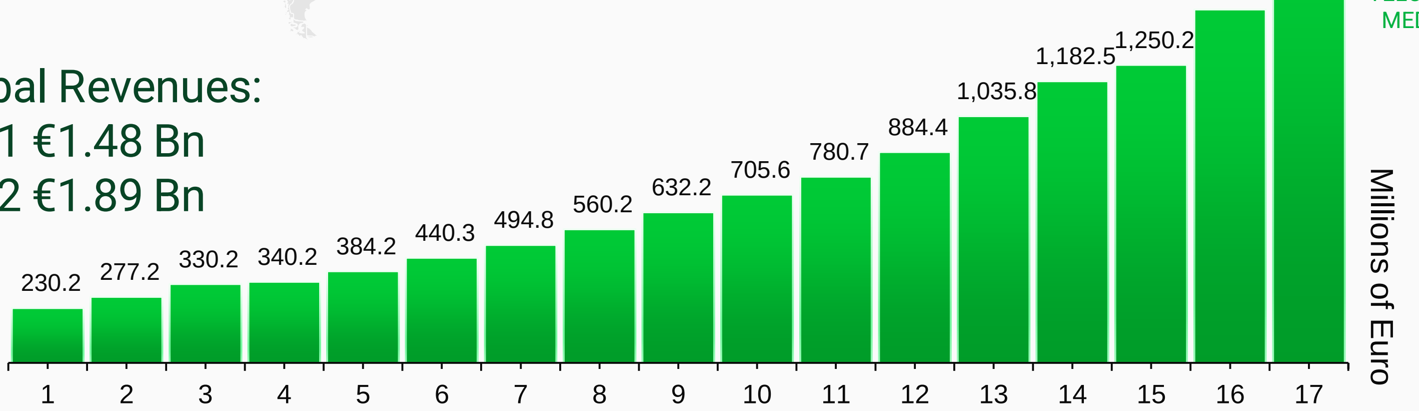
SINGAPORE
Singapore

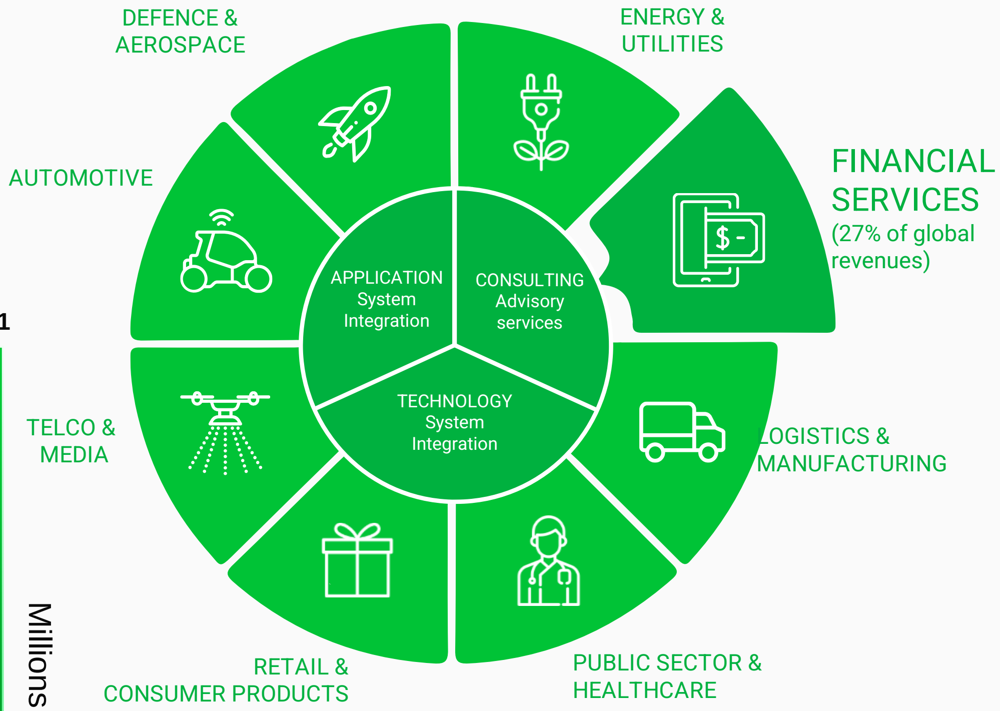
NEW ZEALAND
Auckland

44 Offices across 20 countries

13,500+ Practitioners supporting multiple sectors

Global Revenues:
2021 €1.48 Bn
2022 €1.89 Bn





DEFENCE & AEROSPACE

ENERGY & UTILITIES

AUTOMOTIVE

FINANCIAL SERVICES (27% of global revenues)

TELCO & MEDIA

LOGISTICS & MANUFACTURING

RETAIL & CONSUMER PRODUCTS

PUBLIC SECTOR & HEALTHCARE

APPLICATION System Integration

CONSULTING Advisory services

TECHNOLOGY System Integration

Appendix

Structure of Draft RTS 1 & 2 (ICT RMF) – List of Articles: Title I

Chapter I. ICT SECURITY POLICIES, PROCEDURES, PROTOCOLS, AND TOOLS	
1. General elements of ICT security	11. Data and system security
2. Provisions of governance	12. Logging
3. ICT risk management	13. Network security management
4. ICT asset management policy	14. Securing information in transit
5. ICT asset management procedure	15. ICT project management
6. Encryption and cryptographic controls	16. ICT systems acquisition, development, and maintenance
7. Cryptographic key management	17. ICT change management
8. ICT operating policies and procedures	18. Physical and environmental security
9. Capacity and performance management	19. ICT and information security awareness and training
10. Vulnerability and patch management	

Chapter II. HUMAN RESOURCES POLICY AND ACCESS CONTROL	
20. Human resources policy	22. Access control
21. Identity management	

Chapter III. ICT-RELATED INCIDENT DETECTION AND RESPONSE	
23. ICT-related incident management policy	24. Anomalous activities detection and criteria for ICT-related incidents detection and response

Chapter IV. ICT BUSINESS CONTINUITY MANAGEMENT	
25. Components of the ICT business continuity policy	27. ICT response and recovery plans
26. Testing of the ICT business continuity plans	

Chapter V. REPORT ON THE ICT RISK MANAGEMENT FRAMEWORK REVIEW
28. Format and content

Chapter VI. PROPORTIONALITY PRINCIPLE
29. Complexity and risk considerations

Source: Joint Consultation on the First Batch of DORA Policy Products

Structure of Draft RTS 1 & 2 (ICT RMF) – List of Articles: Title II - Simplified

Chapter I. SIMPLIFIED ICT RISK MANAGEMENT FRAMEWORK	
30. Governance and organisation	33. ICT risk management
31. Information security policy and measures	34. Physical and environmental security
32. Classification of information assets and ICT assets	

Chapter II. FURTHER ELEMENTS OF SYSTEMS, PROTOCOLS, AND TOOLS TO MINIMISE THE IMPACT OF ICT RISK	
35. Access Control	38. ICT security testing
36. ICT operations security	39. ICT systems acquisition, development, and maintenance
37. Data, System and Network Security	40. ICT project and change management

Chapter III. ICT BUSINESS CONTINUITY MANAGEMENT	
41. Components of the ICT business continuity plan	42. Testing of business continuity plans

Chapter IV. REPORT ON THE REVIEW OF THE ICT RMF
43. Format and content

Source: Joint Consultation on the First Batch of DORA Policy Products

Structure of Draft RTS 3 (Criteria for Classification of Incidents) – List of Articles

Section I. CLASSIFICATION CRITERIA
1. Classification criterion ‘Clients, financial counterparts and transactions’ in accordance with Article 18(1) point (a) of Regulation (EU) 2022/2554
2. Classification criterion ‘Reputational impact’ in accordance with Article 18(1)(a) of Regulation (EU) 2022/2554
3. Classification criterion ‘Duration and service downtime’ in accordance with Article 18(1)(b) of Regulation (EU) 2022/2554
4. Classification criterion ‘Geographical spread’ in accordance with Article 18(1)(c) of Regulation (EU) 2022/2554
5. Classification criterion ‘Data losses’ in accordance with Article 18(d) of Regulation (EU) 2022/2554
6. Classification criterion ‘Critical services affected’ in accordance with Article 18(1)(e) of Regulation (EU) 2022/2554
7. Classification criterion ‘Economic impact’ in accordance with Article 18(1)(f) of Regulation (EU) 2022/2554

Section II. MAJOR INCIDENTS AND THEIR MATERIALITY THRESHOLDS AND SIGNIFICANT CYBER THREATS
8. Major incidents in accordance with Article 19(1) of Regulation (EU) 2022/2554
9. Materiality thresholds for the classification criterion ‘Clients, financial counterparts and transactions’
10. Materiality thresholds for the classification criterion ‘Reputational impact’
11. Materiality thresholds for the classification criterion ‘Duration and service downtime’
12. Materiality thresholds for the classification criterion ‘Geographical spread’
13. Materiality thresholds for the classification criterion ‘Data losses’
14. Materiality thresholds for the classification criterion ‘Critical services affected’
15. Materiality threshold for the classification criterion ‘Economic impact’
16. Recurring incidents
17. Criteria and high materiality thresholds for determining significant cyber threats

Section III. RELEVANCE OF MAJOR INCIDENTS IN OTHER MEMBER STATES AND DETAILS TO BE REPORTED TO OTHER COMPETENT AUTHORITIES
18. Relevance of major incidents to competent authorities in other Member States
19. Details of major incidents to be reported in accordance with Article 19(6) and (7)

Source: Joint Consultation on the First Batch of DORA Policy Products

Structure of Draft RTS 4 (Policy on Services by ICT TPPs) – List of Articles

Main Articles
1. Complexity and risk considerations
2. Group application
3. Governance arrangements regarding the policy on the use of ICT services supporting critical or important functions
4. ICT third-party service providers and ICT services supporting critical or important functions
5. Main phases of the life cycle for the use of ICT services supporting critical or important functions provided by ICT third- party service providers
6. Ex-ante risk assessment
7. Due diligence
8. Conflict of interest
9. Contractual clauses for the use of ICT services supporting critical or important functions
10. Monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions
11. Exit and termination of contractual arrangements for the use of ICT services supporting critical or important functions
12. Entry into force

Source: Joint Consultation on the First Batch of DORA Policy Products

Structure of Draft ITS (Register of Information Templates) – List of Articles

Chapter I. SUBJECT MATTER AND DEFINITIONS
1. Subject matter
2. Definitions
3. Data points requirements

Chapter II. REGISTER OF INFORMATION AT ENTITY LEVEL
4. General requirements for maintaining and updating the register of information at entity level
5. Content of the register of information maintained and updated at entity level

Chapter III. REGISTER OF INFORMATION ON SUB-CONSOLIDATED AND CONSOLIDATED LEVEL
6. Responsibility for maintaining and updating register of information at sub-consolidated and consolidated level
7. Additional requirements for maintaining and updating the register of information at sub-consolidated and consolidated level
8. Content of the register of information maintained and updated at sub-consolidated and consolidated level

Chapter IV. AVAILABILITY OF THE REGISTER OF INFORMATION
9. Access of the competent authorities to the Registers of Information

Chapter V. FINAL PROVISIONS
10. Entry into force

Source: Joint Consultation on the First Batch of DORA Policy Products