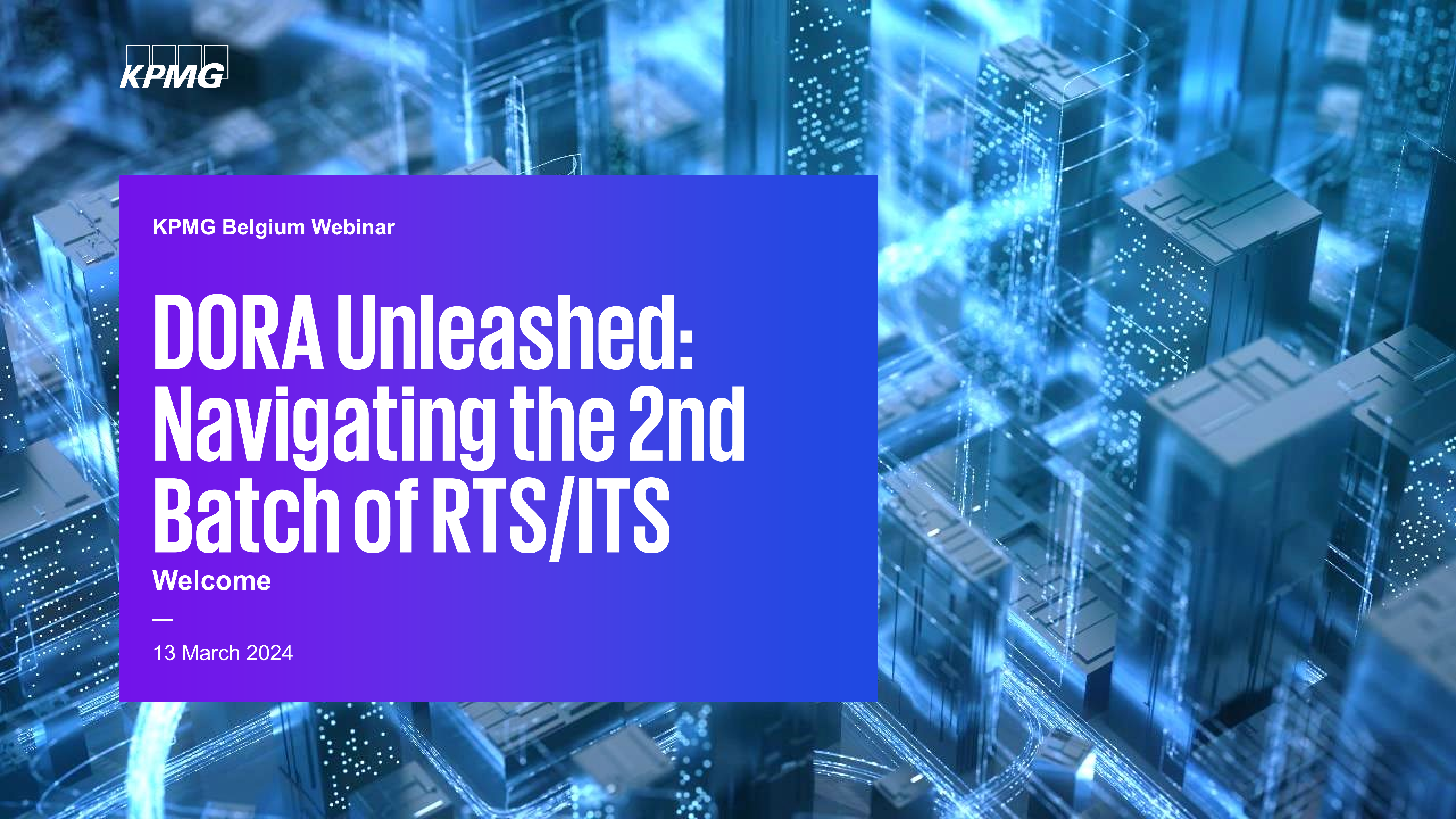


KPMG Belgium Webinar

DORA Unleashed: Navigating the 2nd Batch of RTS/ITS

Welcome

—

13 March 2024

Today's Speakers

Benny Bogaerts

Introduction

Benoit Watteyne

DORA Status

DORA Benchmark

Thomas Meyer

DORA RTS/ITS Batch 1 Update

DORA RTS/ITS Batch 2 Update

Sonia Rosu

RTS/ITS Incident Reporting

Peter Vanderheyden

RTS TLPT

Kris Vancolen

DORA & Operational Risk

Our KPMG DORA EMA Network

Our **KPMG EMA DORA Network** combines our **local expertise**, brings together our **wide-range of benchmark experiences** and allows us to compare and develop **best practices**. By utilizing our EMA network, **we can offer efficient and targeted solutions to meet DORA requirements while maintaining the highest quality standards.**

Vaike Metzger
EMA Lead | Partner

Karri Tomula
Director

Sophia Hauswurz
Manager

Søren K. Lauritzen
Senior Manager

Mikael Johannesen
Director

Nicklas Wallenborg
Director

Ali Alam
Senior Manager

Augustinus Mohn
Senior Manager

Fayçal El Belghami
Partner

Benny Bogaerts
Partner

Laurent de la Vaissière
Partner

Luca Boselli
Partner

Juan de Dios Lechuga
Partner

Cristina Alberto
Director

Andreas Tomek
Partner

Marcin Kieszkowski
Senior Manager

Michał Kurek
Partner

Theodoros Stergiou
Director

Diarmuid Curtin
Director

Ivar Anton
Senior Manager

Gheorghe Vlad
Director

Lukács Kornél
Partner

Andreas Rieber
Executive Director

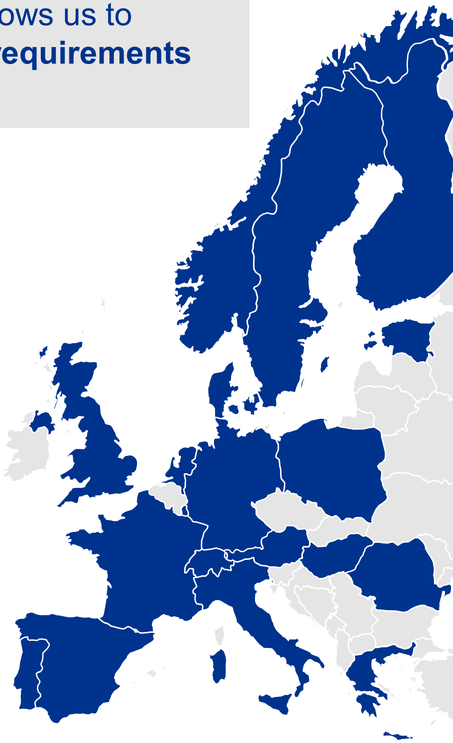
Sebastien Fix
Director

Elena Silanteva
Senior IT Advisor

Marija Devic
Director

Indy Dhami
Partner

Mihai Rada
Partner



Further working group leader

- Ali Lam, Cyber
- Caroline Sieveritz, TPRM
- Jordi van den Breekel, TLPT

- Andrew VanWagoner, ServiceNow
- Stefanie Fekonja, BCM
- Julian Dersch, JIRA

Extended DORA network

DORA Recap

Governance requirements

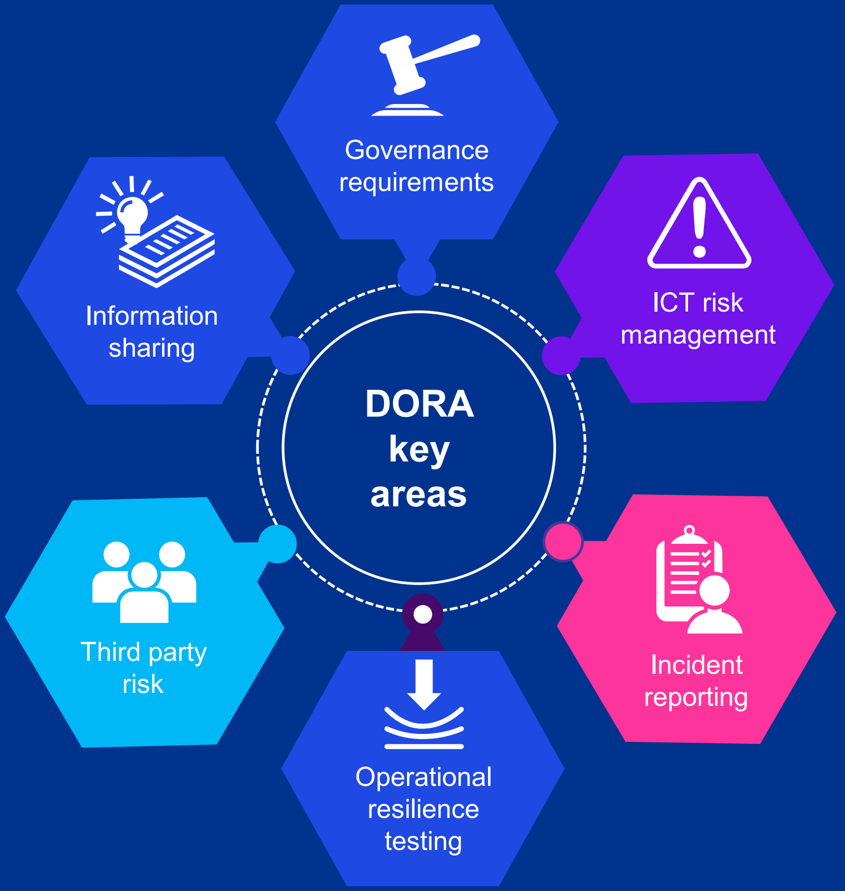
Internal controls and governance structure

Information sharing

Exchange of cyber threat information and intelligence

Third party risk

Risk systems and tools to cover third parties risk and supervision



ICT risk management

ICT risk system and tools, including business continuity and disaster recovery

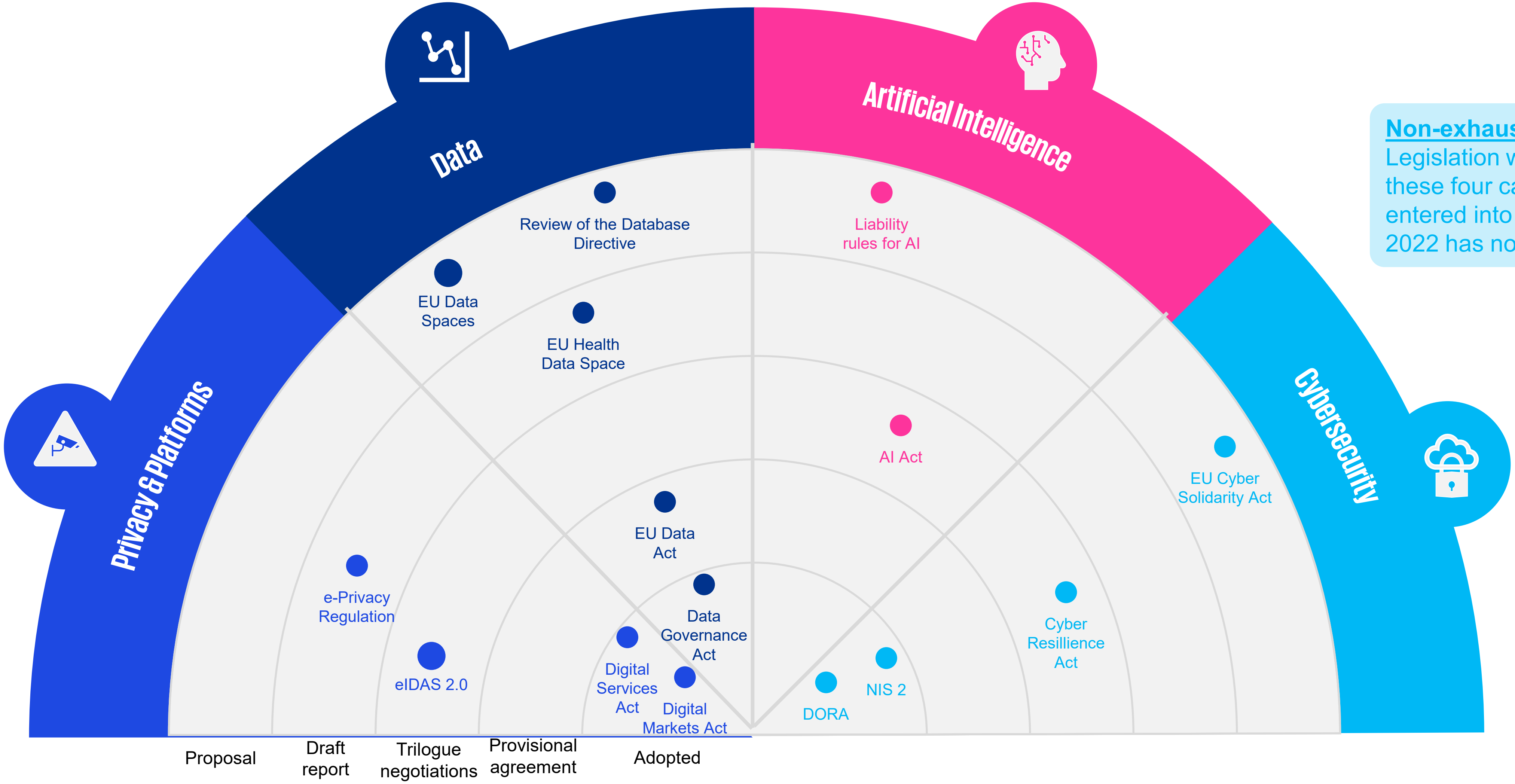
Incident reporting

Reporting thresholds and systems to communicate to regulators and users

Operational resilience testing

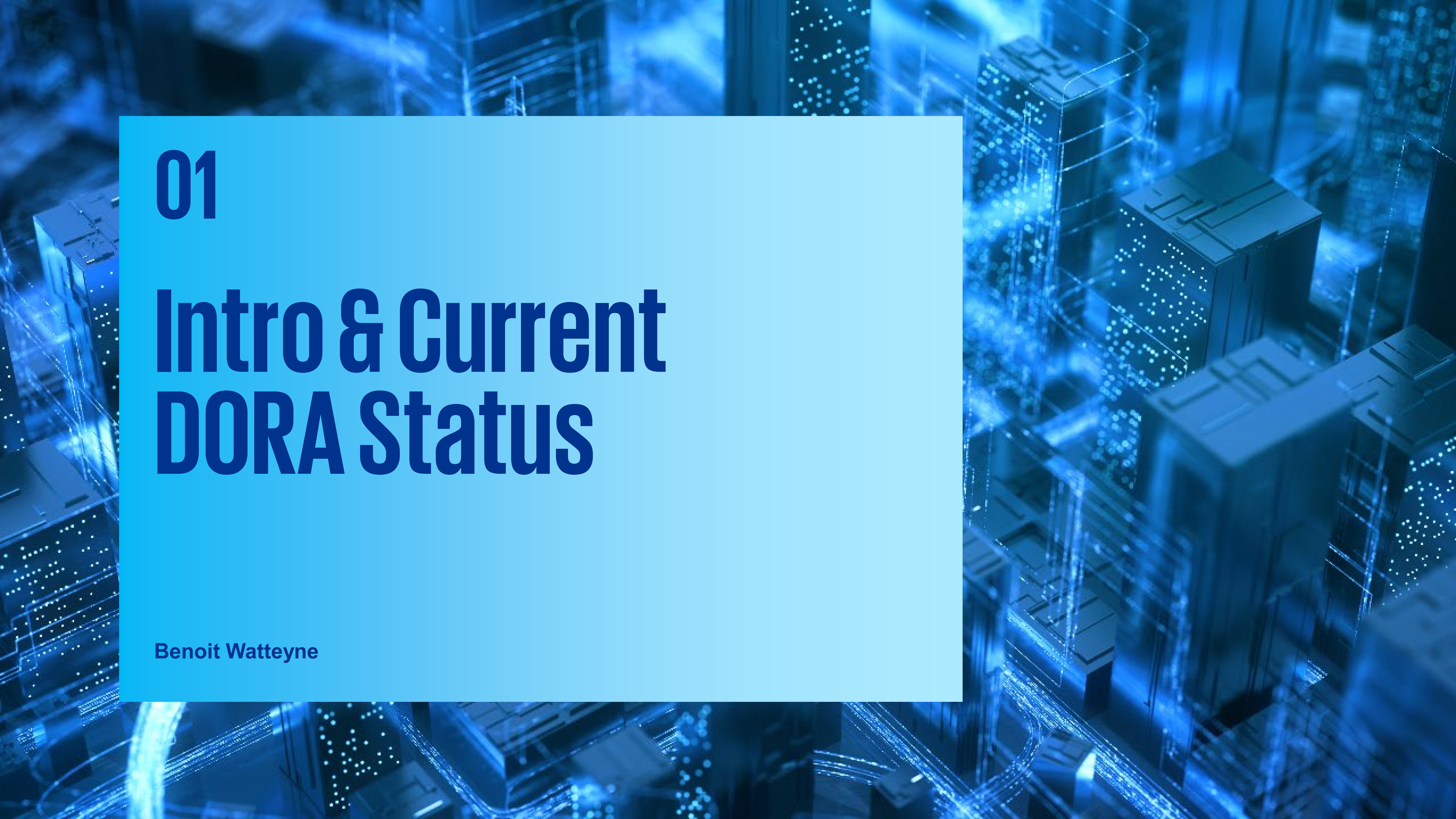
Testing for preparedness and weakness identification

Upcoming Legislative Initiatives Digital Single Market Package



Non-exhaustive

Legislation which does not fall into these four categories, or which entered into force before October 2022 has not been included.

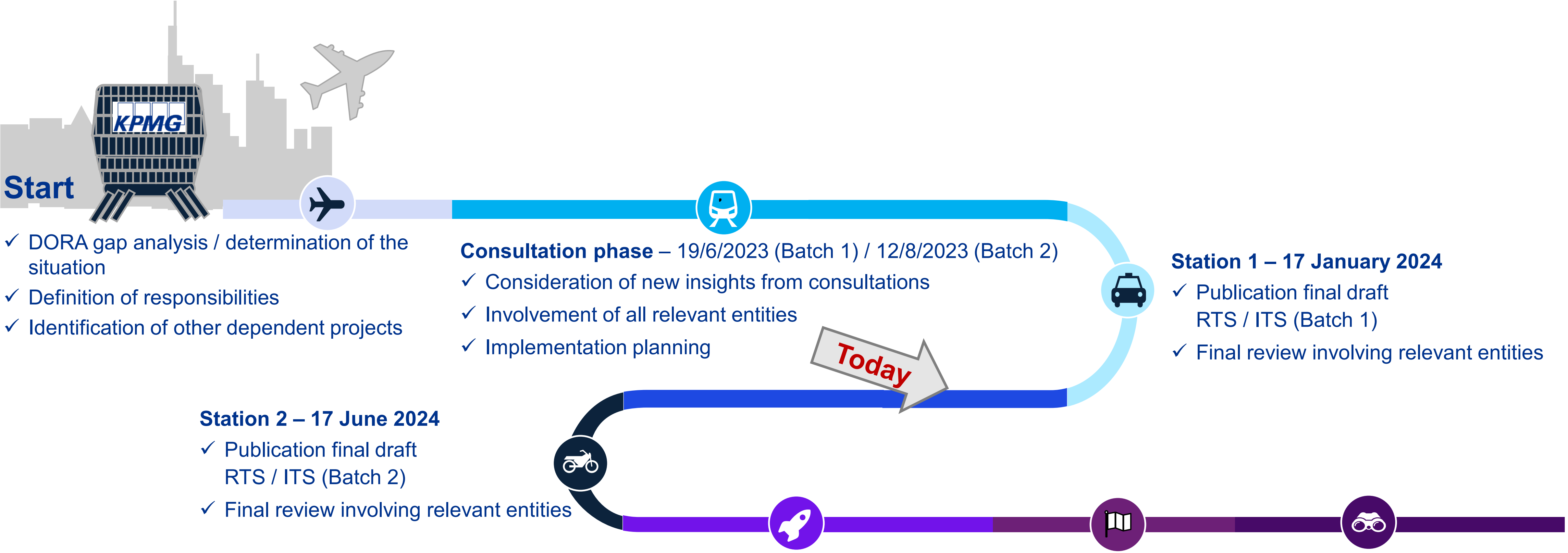


01

Intro & Current DORA Status

Benoit Watteyne

Status quo



Start

- ✓ DORA gap analysis / determination of the situation
- ✓ Definition of responsibilities
- ✓ Identification of other dependent projects

Consultation phase – 19/6/2023 (Batch 1) / 12/8/2023 (Batch 2)

- ✓ Consideration of new insights from consultations
- ✓ Involvement of all relevant entities
- ✓ Implementation planning

Station 1 – 17 January 2024

- ✓ Publication final draft RTS / ITS (Batch 1)
- ✓ Final review involving relevant entities

Station 2 – 17 June 2024

- ✓ Publication final draft RTS / ITS (Batch 2)
- ✓ Final review involving relevant entities

Sprint - Final implementation phase

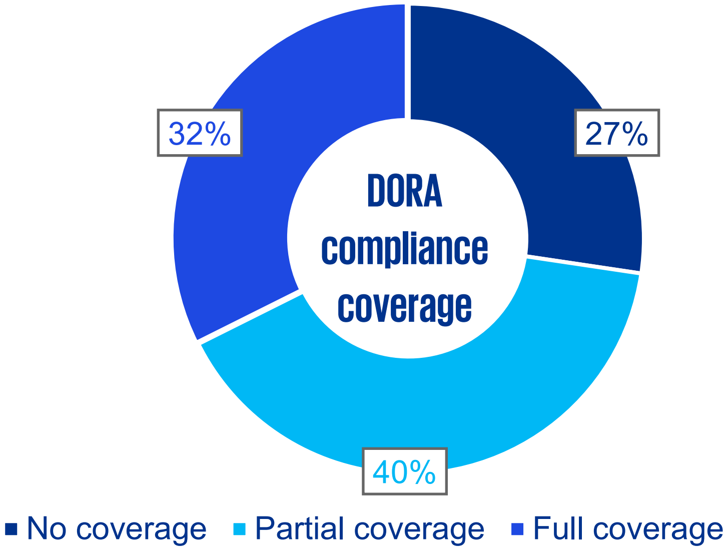
- ✓ Implementation support
- ✓ Possible start of preparation for first DORA supervisory examinations (OSI)

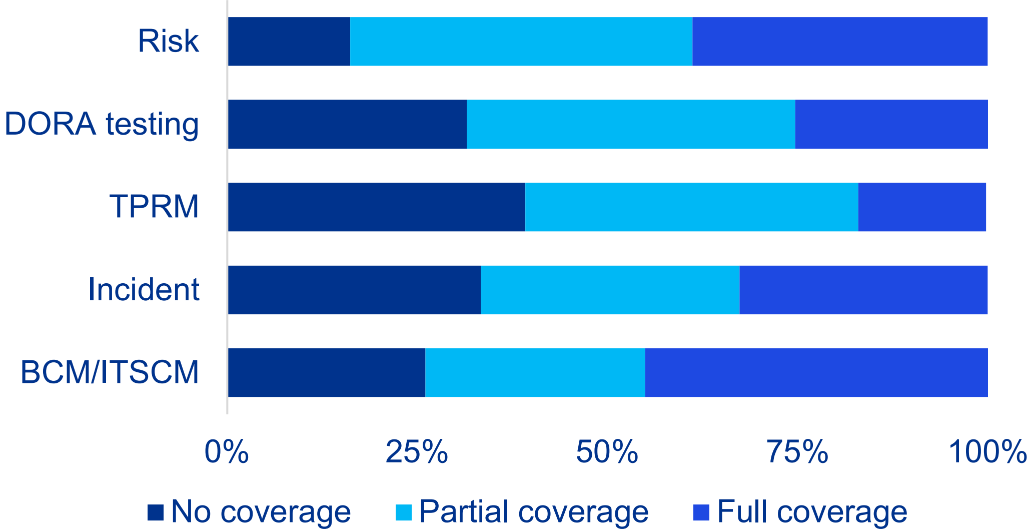
17 January 2025
Goal
DORA compliance

Outlook

- ✓ OSI-preparation
- ✓ DORA in FSA (in discussion, national decision)

Action is required to be fully compliant for over two thirds of DORA requirements



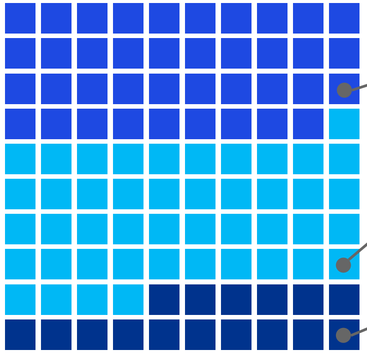


Overarching insights

Existent IT Governance, Frameworks, Controls and Policies can provide a baseline for the greater expansion for DORA compliance. While striving for DORA compliance, a holistic approach must be applied.

- Current risk management frameworks may be utilized as foundation for DORA improvements, as 39% of risk related DORA requirements are mostly fulfilled.
- Call for action for TPRM: Information register are in most cases not fully DORA compliant.
- Size matters! No coverage is two times more likely for companies with less than 1 Mio. EUR in revenue.
- Due to more applicable regulations, international business operations usually fulfil ~50% of DORA requirements already.

In ‘Risk’ initial compliance coverage can be utilized as a baseline to further improve in a holistic manner



39% **Full Coverage**
Simplified ICT risk management frameworks (II.16) are mostly established.
Requirements on ICT systems, protocols and tools (II.7) either fully or partially fulfilled.

45% **Partial Coverage**
40% of Identification (II.8) and communication (II.14) as well as Governance and organization (II.5) related requirements are already covered partly.

16% **No Coverage**
Learning and evolving (II.13) are one of the major improvement areas as well as further ICT risk management framework (II.6) related enhancements.

Risk Management Framework

Missing DORA compliant holistic ICT risk management framework.

✓ Integrate overall governance in one consolidated ICT risk management framework.

Continual Improvement

Missing monitoring capabilities for continues learning and evolving.

✓ Ensure resources & monitoring by default to enable analysis of ICT risk over time.

Detection & Prevention

Insufficient documentation of ICT supported business functions.

✓ Annually review documentation of ICT supported functions and assets

Information Security

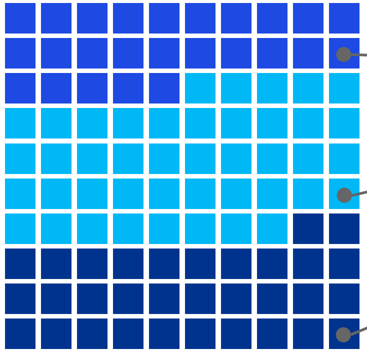
Partly insufficiently implemented required security measures

✓ Review and adjust security measures required by security policies and adapt accordingly.

Existent regulatory requirements are not extending beyond standard risk management processes.

A holistic approach with an integrated Risk Management Framework and Strategy covering all ICT functions and ICT assets must be implemented. ✓

In 'DORA Testing' an overarching testing concept considering threat scenarios may be implemented covering all ICT assets



25% **Full Coverage**
Initial testing programs with sufficient resources and at minimum frequency (IV.24) may be used as a foundation for further expansion for DORA testing.

43% **Partial Coverage**
General requirements for DOR testing (IV.24) for majority at least partly fulfilled. Test types per DORA IV.25 sub article 1 are at least partly already used.

32% **No Coverage**
Advanced testing of ICT tools, systems and processes based on TLPT (IV.26) and implementing requirements for testers for TLPT (IV.27) are major improvement areas.

Overall Testing

Insufficient scope of testing or too unmethodological approach to testing.

✓ Overarching testing concept including derivation of test cases based on threats and full coverage of ICT assets.

Threat Led Penetration Testing

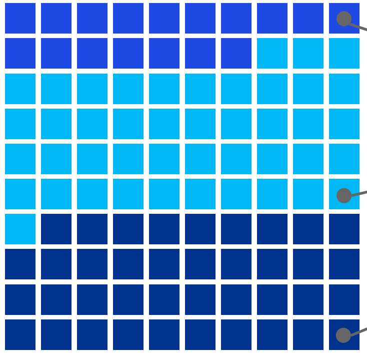
Lack of overall TLPT requirements regarding conducting TLPT and TLPT testers.

✓ Concept for TLPT also documenting required expertise for conducting TLPT.

Current testing procedures mostly cover planned recovery or emergency procedures and are not derived through threats.

All ICT assets must be covered through a regular, methodological approach to testing by deriving test cases through threat scenarios and implementing lessons learned. ✓

In 'TPRM' a strategic approach to third-party risk needs to be combined with a readily available information register



17% **Full Coverage**
General principles before entering a contractual arrangement on the use of ICT services (V.28.4) are mostly already covered or at least partly covered.

44% **Partial Coverage**
Exit strategies (V.28) are in most cases existent, but do not fulfill all relevant DORA requirements – same applies to the exercise of access, inspection and audit rights.

39% **No Coverage**
Biggest challenges arise from maintaining a DORA compliant information register (V.28), using DORA compliant contracts (V.30) and establishing a TPRM function

Contracts

No proper handling of subcontracting and contractual agreements (incl. Exit).

✓ Leverage mandatory standardized contractual clauses in every contract with ICT service providers.

Strategy/Governance

Missing TPRM function and pre-determined audit planning.

✓ Integrate a TPRM function in the governance as part of the ICT risk management framework.

Information Register

No comprehensive, up to date register of information with proper consolidation.

✓ Integrate a readily available register of information within the overall CMDB and information domain.

Risk Analysis

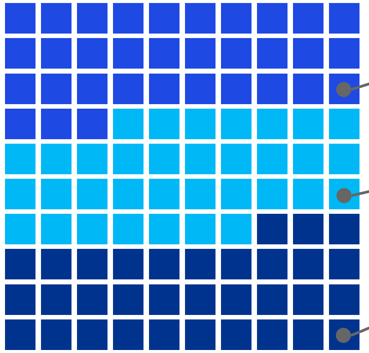
Insufficient management of ICT risk concentration as part of the ICT third-party risk strategy.

✓ Embed preliminary risk assessments in the ICT risk management framework to avoid concentration risks.

Ad-hoc reporting duties and standardized contractual clauses with ongoing oversight requirements expand beyond the existent.

Implement a TPRM function within the ICT risk management framework while leveraging standardized contracts and a tool-enabled information register. ✓

In 'Incident' a methodological approach needs to tackle response management, communication and classification



33% **Full Coverage**
Basic ICT-related incident management processes (III.17) and initial detection capabilities for anomalies, incidents and cyber threats (II.10) are implemented.

34% **Partial Coverage**
Classification of ICT-related incidents (III.18) is in no instance comprehensively done. Learning and evolving (II.13) is not deeply enough embedded in the overall processes.

33% **No Coverage**
Reporting on major ICT-related incidents (III.19) in a timely manner is either not foreseen as part of processes or not possible due to a lack of technical capabilities.

Response Management

Incident processes are immature and not properly with threat intelligence intertwined.

✓ Set-up holistic ICT-related incident management processes with early warning and notification capabilities.

Communication Strategies

Insufficiently implemented communications strategy and according governance.

✓ Establish incident response team and communication strategy alongside ICT risk management framework.

Classification of ICT related Incidents

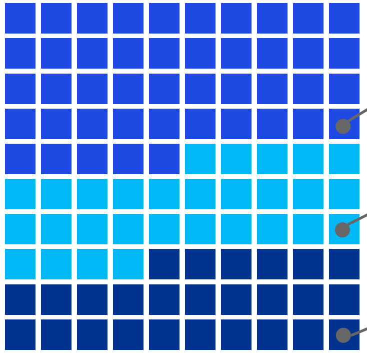
Classification of ICT-related incidents and cyber threats not properly implemented.

✓ Derive and implement criteria for classification in a methodological and tool-based manner.

Classification criteria and reporting duties are increasing the need for automated and integrated solutions.

Tool-based ICT-related incident classification with interfaces for threat intelligence and reporting and notification capabilities in one place. ✓

In 'BCM/ITSCM' existent methodologies for BCM / ITSCM and backup may be leveraged for DORA compliance



45% **Full Coverage**
Business Continuity Plans (II.11.4), Business Impact Analysis (II.11.5) and a Crisis Management (II.11.7) are oftentimes already established and conducted.

29% **Partial Coverage**
The ICT business continuity policy (II.11.2) is at least partly in most instances implemented while also being partly tested (II.11.6).

26% **No Coverage**
Segregation of backup systems from source systems, proper protection of backup systems and integrity checks in data recovery are lacking proper implementation (II.12).

BCM

Lack of records before and during business continuity plan activation.

✓ Implement tool-based record management system while leveraging existent implementations.

ITSCM

Insufficient test of BCPs also covering cyber-attacks and ICT infrastructure switchover.

✓ Conduct regular and comprehensive business continuity and incident response exercise

Backup systems

Inappropriate set-up of backup systems and their periodic testing.

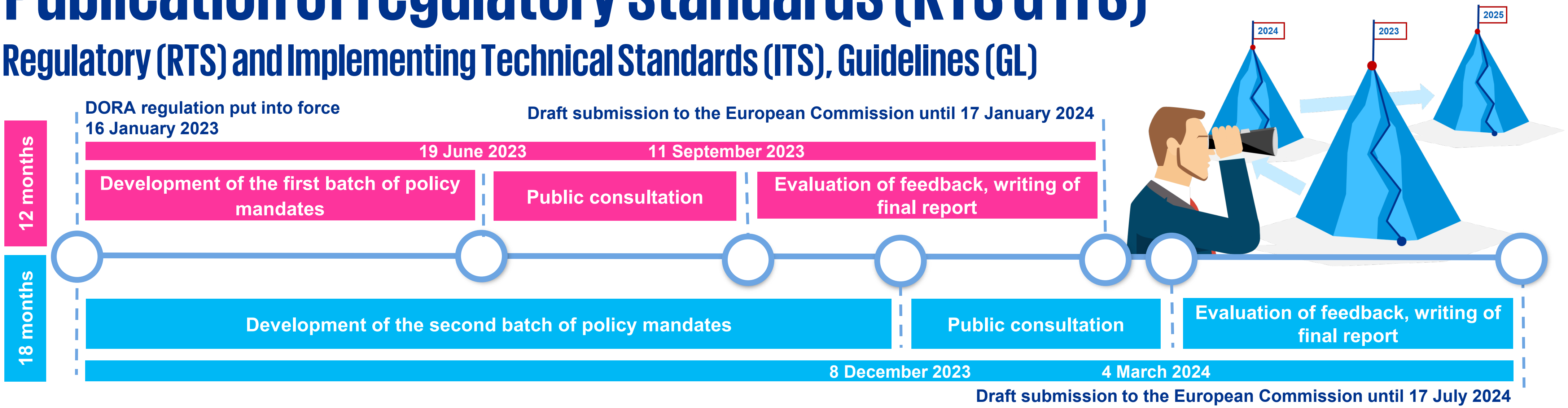
✓ Policy for data backup and recovery incl. testing and secure data backup system set-up.

Testing scope and requirements for backup system security and segregation are not fully covered through existent requirements.

Implement security and segregation by design for data backup. Introduce tool-based record keeping and plan for comprehensive ITSCM tests.✓

Publication of regulatory standards (RTS & ITS)

Regulatory (RTS) and Implementing Technical Standards (ITS), Guidelines (GL)



12 months

DORA regulation put into force
16 January 2023

Draft submission to the European Commission until 17 January 2024

19 June 2023

11 September 2023

Development of the first batch of policy mandates

Public consultation

Evaluation of feedback, writing of final report

18 months

Development of the second batch of policy mandates

Public consultation

Evaluation of feedback, writing of final report

8 December 2023

4 March 2024

Draft submission to the European Commission until 17 July 2024

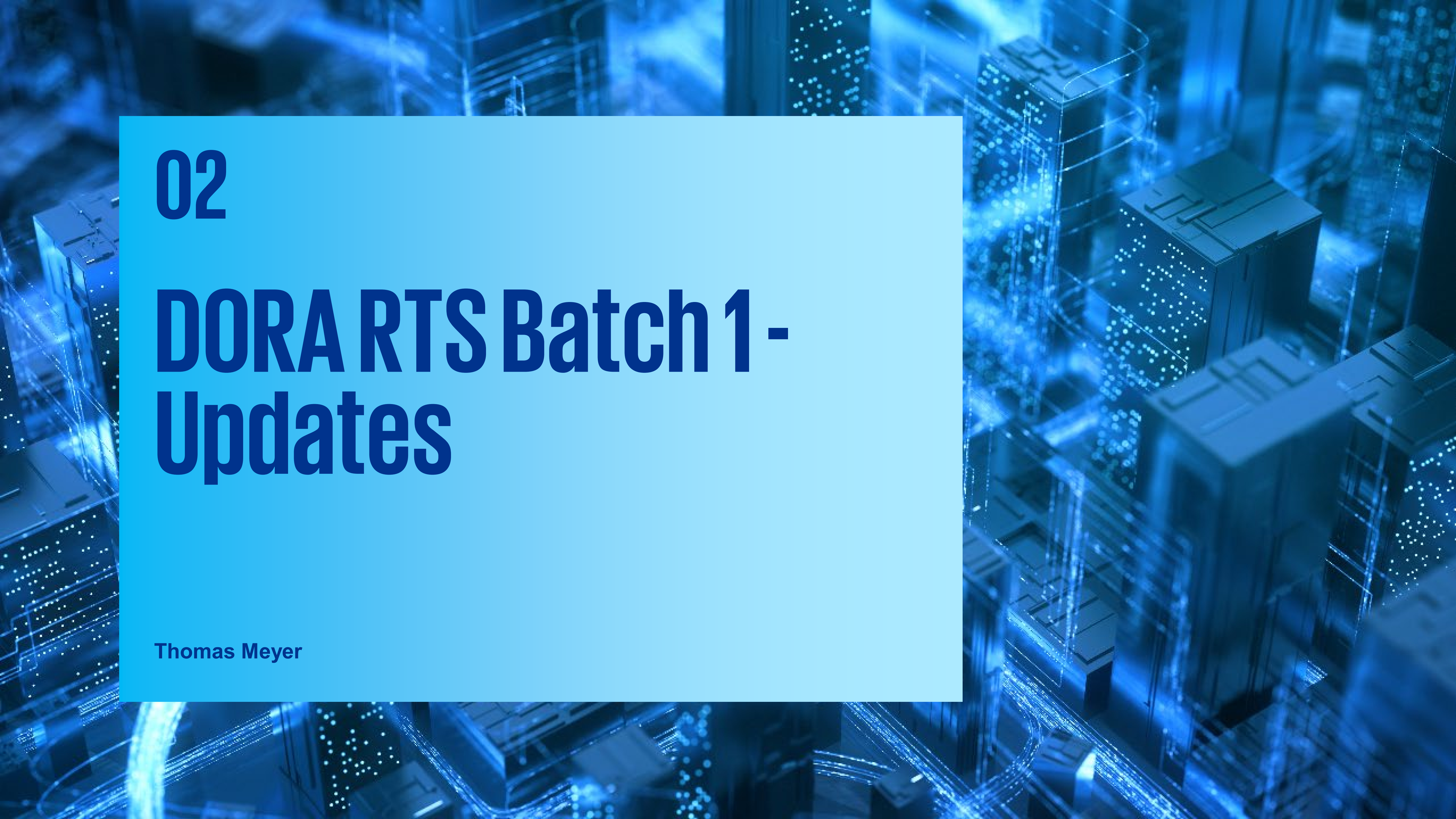
ICT risk management framework (Chapter II)	ICT- related incident management, classification and reporting (Chapter III)	Testing digital operational resilience (Chapter IV)	ICT third party risk management. (Chapter V Section I)	Monitoring framework (Chapter V Section II)
🔴 RTS for ICT- risk management framework (Art.15) 🔴 RTS for the simplified ICT risk management framework (Art.16.3) 🔵 GL on the estimation of aggregated annual costs and losses (Art.11.1)	🔴 RTS for classification of ICT-related incidents and cyber threats (Art.18.3) 🔵 RTS for the content of the reports of major ICT- related incidents (Art.20.a) 🔵 ITS for the reporting standards for a financial entity to report a major incident (Art.20.b) ⚫ Feasibility of further centralization of major incident reporting through a single EU- Hub (Art.21) Draft submission until 17 January 2024	🔵 RTS for advanced testing of ICT tools, systems and processes based on TLPT (Art.26.11)	🔴 ITS with standard templates for the purposes of the register of information (Art.28.9) 🔴 RTS to further specify the detailed content of contractual arrangements (Art.28.10) 🔵 RTS for subcontracting ICT services supporting critical or important functions (Art.30.5)	⚫ EC seeks ESAs' opinion on criticality criteria (Art.31.6) and oversight fees (Art.43.2) Draft submission until 17 July 2024 🔵 GL for cooperation between the ESAs and the competent authorities (Art.32.7) 🔵 RTS for harmonization of the oversight activates (Art.41)

🔴 First batch of policy products

🔵 Second batch of policy products

⚫ Other policy instruments

KPMG



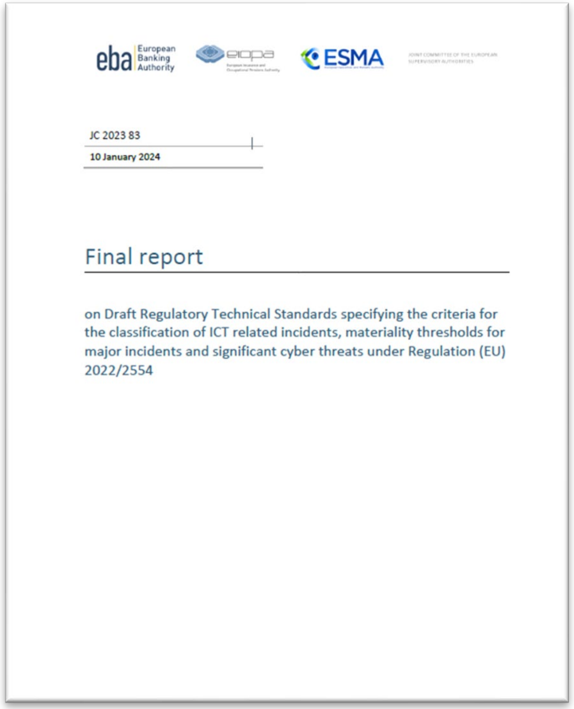
02

DORA RTS Batch 1 - Updates

Thomas Meyer

DORA RTS Batch 1 - Finalization

17 January 2024: ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification



JC 2023 83

10 January 2024

Final report

on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

RTS – Criteria for the classification of ICT related incidents

JC 2023 86

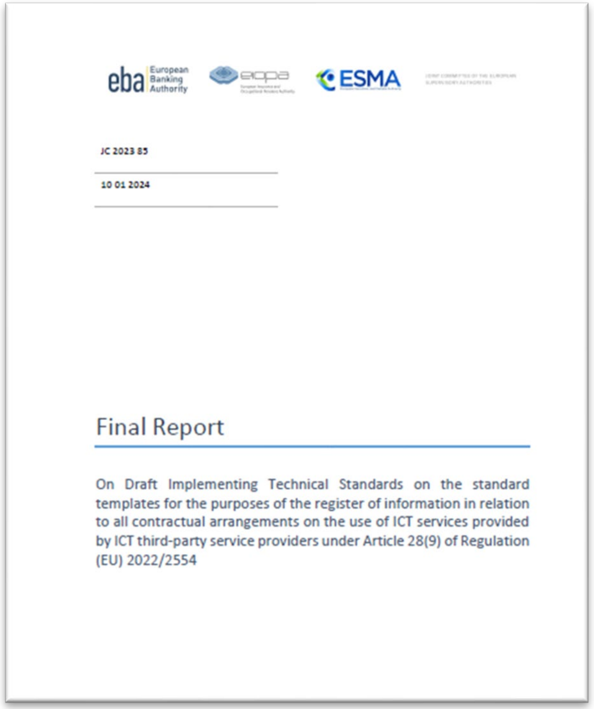
10 01 2024

Final report

Draft Regulatory Technical Standards

to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

RTS – ICT risk management, tools, processes and policies



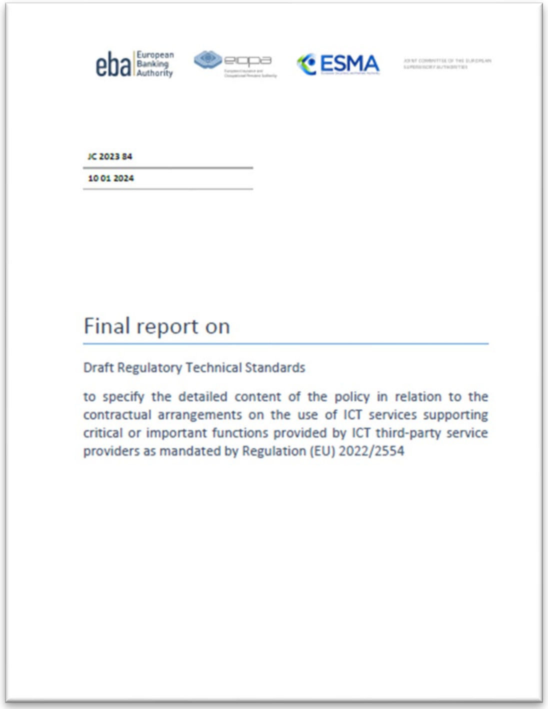
JC 2023 85

10 01 2024

Final Report

On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

ITS – ICT risk management, tools, processes and policies



JC 2023 84

10 01 2024

Final report on

Draft Regulatory Technical Standards

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 as mandated by Regulation (EU) 2022/2554

RTS – Contractual arrangements for supporting ICT services

Final draft RTS on ICT Risk Management Framework

Final draft RTS on ICT Risk Management Framework consists of the following updates:

- Textual updates
- Restructuring
- Clarification in scoping
- Additional requirements
- Classification/scoping based on DORA or existing regulations
- (Partially) scrapped

JC 2023 86

10 01 2024

Final report

Draft Regulatory Technical Standards

to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

Updated

Clarification of scoping (1/3)

Article 7 – Cryptographic key management

Sub-article 4

Old:

Financial entities shall create and maintain a register for *all certificates and certificate storing devices*. The register shall be kept up-to date.

New:

Financial entities shall create and maintain a register for *all certificates and certificate storing devices for at least ICT assets supporting critical or important functions*. The register shall be kept up-to-date.

Scoping is clarified to maintaining all certificates and certificate storing devices of for at least ICT assets that support critical or important functions.

Updated

Clarification of scoping (2/3)

Article 13 – Network security management

Sub-article 1 – clause M

Old:

with reference to network services agreements, the identification and definition of ICT and information security measures, service levels and management requirements of all network services, whether these services are provided *in-house or outsourced*

New:

with reference to network services agreements, the identification and definition of ICT and information security measures, service levels and management requirements of all network services, whether these services are provided by *an ICT intra-group service provider or by ICT third-party service providers*

Scoping is clarified as in practice in-house often means intra-group delivered services as well.

Updated

Clarification of scoping (3/3)

Article 26 – ICT response and recovery plans

Sub-article 4

Old:

As part of the ICT response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers which are of *key importance for a financial institution's ICT service continuity*.

New:

As part of the ICT response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers of ICT services *supporting critical or important functions to the financial entity.*

The initial terminology "key importance" is potentially subject to interpretation, therefore changed to main premise of DORA through "critical and important functions".

Added

Additional requirements (1/2)

01

Article 7 – Cryptographic key management

Sub-article 5

Financial entities shall ensure the **prompt renewal of certificates** in advance of their expiration.

02

Article 8 – Policies and procedures for ICT operations

Sub-article 2 – clause B

Two additional requirements:

- (vi) requirements to conduct the **development and testing** in environments which are **separated from the production environment**
- (vii) requirements to conduct the **development and testing in production** environments. The policies and procedures shall provide that the instances in which testing is performed in production environment are **clearly identified, justified, for limited periods of time approved by the relevant function**, and considering Article 16(6). The **availability, confidentiality, integrity and authenticity of ICT systems and production data shall be ensured** during development and test activities in production environment

Added

Additional requirements (2/2)

03

Article 23 – Anomalous activities' detection and criteria for ICT-related incidents' detection and Response

Sub-article 2 – clause A

One additional requirement:

- **ICT-related incident notification from an ICT third-party** service provider of the financial entity **detected in the ICT systems and networks of the ICT third-party service provider** and which may affect the financial entity

Classification/scoping based on DORA or existing regulations (1/2)

Updated

Article 10 – Vulnerability and patch management

Sub-article 2 – clause B

Addition that **”frequency and scope”** of vulnerability scanning and assessment **is dependent on the classification (based on Article 8(1) of DORA)** and the overall risk profile of the ICT asset

Article 12 – Logging

Sub-article 2 – clause C

Addition that logging of events takes into scope:

c) **identity management** in accordance **with Article 20** and **logical and physical access control**, in accordance **with Article 21** of this RTS

Updated

Classification/scoping based on DORA or existing regulations (2/2)

Article 13 – Network security management

Sub-article 1 – clause K

The implementation of a **secure configuration baseline of all network components and hardening the network** and network devices according to vendor instructions, to, where applicable, standards as defined in **Article 2, point (1), of Regulation (EU) No 1025/2012** and leading practices

Article 21 – Access control

Sub-article 1 – clause E, F, i

i) the use of **authentication methods commensurate to the classification** established according to Article 8(1) of Regulation (EU) 2022/2554 and to the overall risk profile of ICT assets and considering leading practices

Regulation (EU) 2022/2554: The Digital Operational Resilience Act

(Partially) Scrapped (1/3)

Deleted

Article 19 – ICT and Information security awareness and training

Fully scrapped.

Reasoning:

A group of stakeholders noted in consultation that this article might not be in scope of the mandate of the draft RTS and the ESAs agree with this feedback. The article has therefore been deleted.

ESAs will consider developing further guidance on this area, as it is considered vital to ensure an effective digital operational resilience.

Elements around roles and responsibilities, awareness of policies and procedures, as well as awareness of reporting mechanisms remain in place.

(Partially) Scrapped (2/3)

Deleted

Article 22 – ICT-related incident management policy

Scrapped: Sub article 1 – clause F:

(f) review and update at least once a year the ICT-related incident management policy, its procedures, protocols, and tools. The ICT response and recovery plans shall be reviewed against a range of different plausible scenarios.

Potential reasoning:

Grant the financial institutions more room to maintain the ICT-related incident management policy in a frequency that aligns better with their internal risk assessment, classifications and scope.

(Partially) Scrapped (3/3)

Deleted

Article 29 Complexity and risk considerations – Proportionality principle

Fully scrapped.

Reasoning:

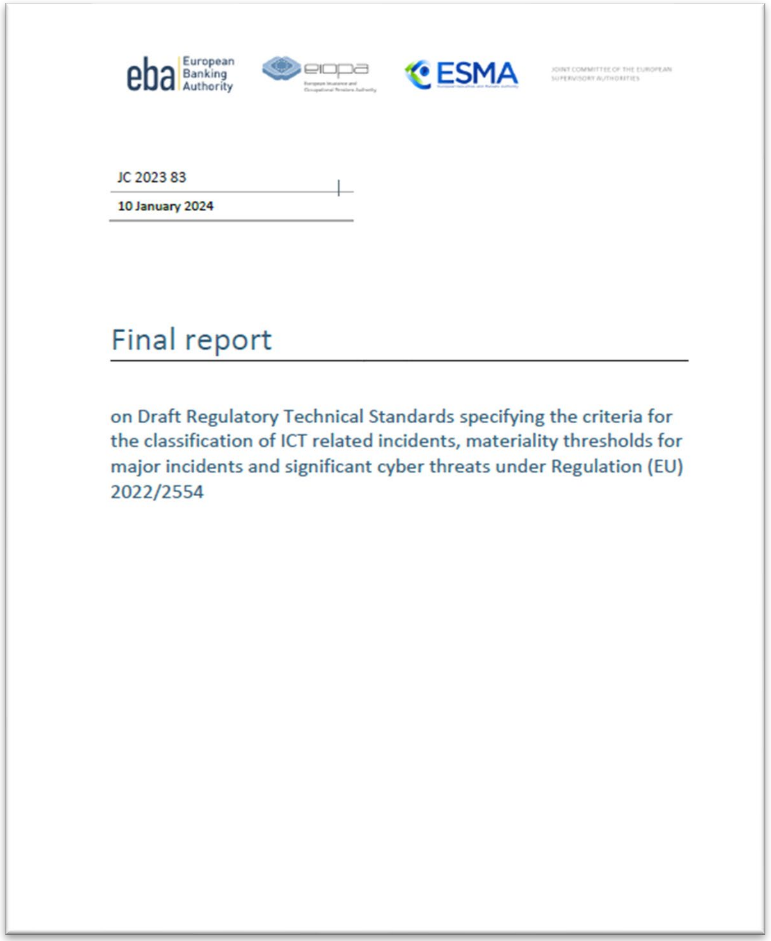
The element of proportionality is already embedded in DORA via multiple routes which include:

- Article 4 of DORA 'Proportionality principle';
- Exemptions for microenterprises from various requirements of Chapter II on ICT risk management;
- Article 16 of DORA 'Simplified ICT risk management framework' for a number of financial entities identified as smaller than the others.
- The draft RTS contains provisions addressed to specific entities that present specific profiles of ICT risks (CCPs, CSDs, trading venues)
- Article 1 of the draft RTS provides for considerations on elements of complexity and increased or reduced overall risk profile in the application of the draft RTS.

Final draft RTS on classification of ICT related incidents

Final draft RTS on classification of ICT related incidents includes the following updates:

- Simplification of ICT incident Classification model
- Further explanation of definitions



JC 2023 83

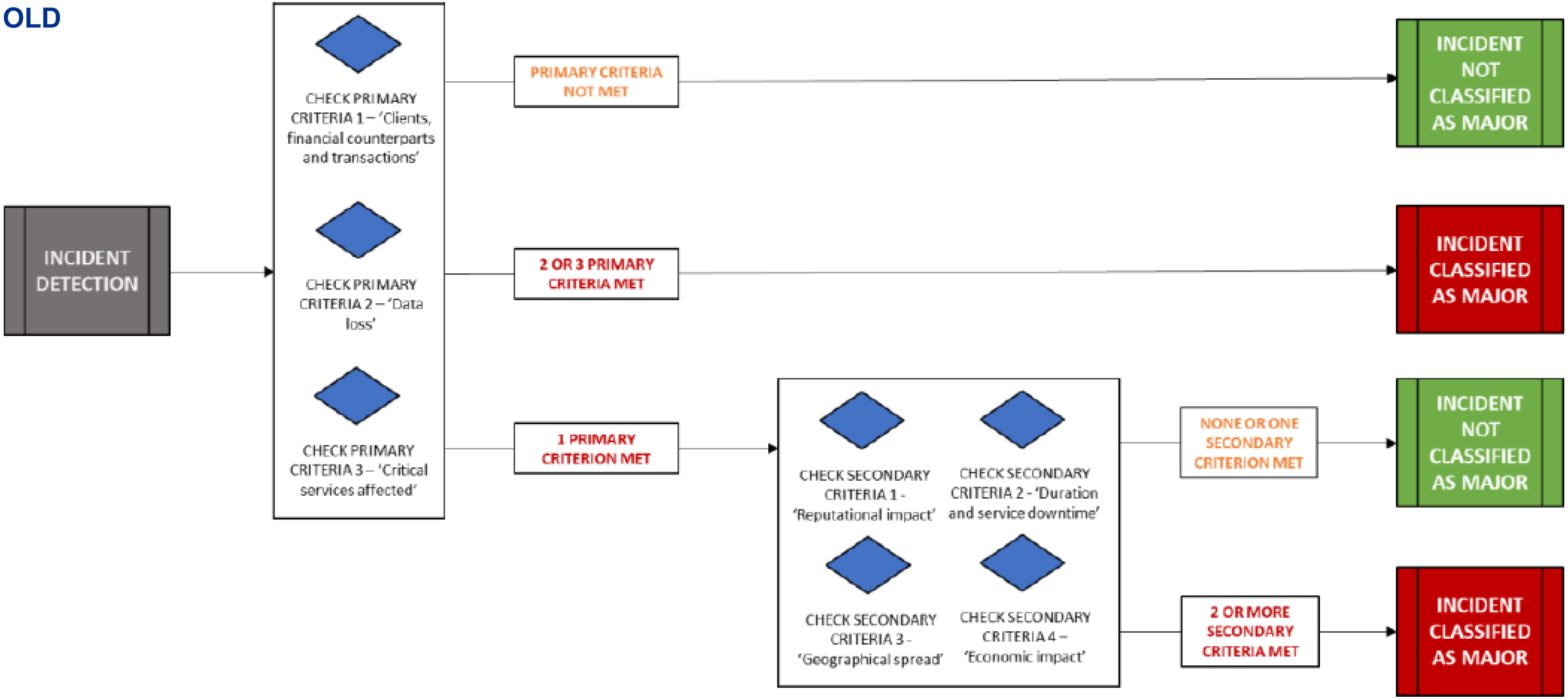
10 January 2024

Final report

on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554

Simplification of ICT incident classification model

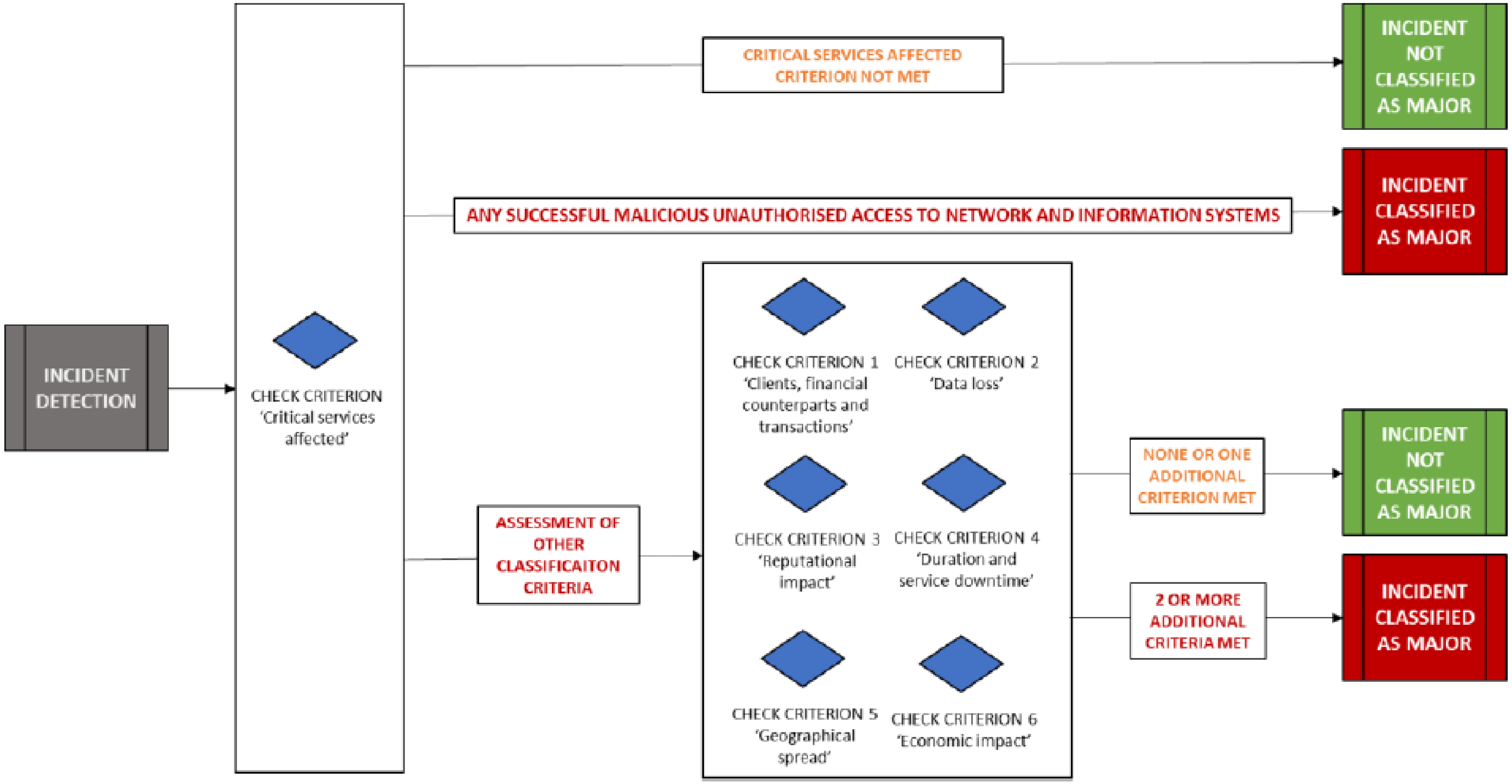
OLD



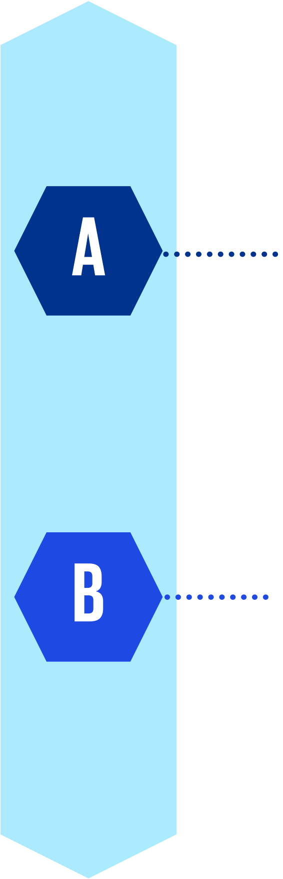
INCIDENT DETECTION
CHECK PRIMARY CRITERIA 1 – 'Clients, financial counterparts and transactions'
CHECK PRIMARY CRITERIA 2 – 'Data loss'
CHECK PRIMARY CRITERIA 3 – 'Critical services affected'
PRIMARY CRITERIA NOT MET
2 OR 3 PRIMARY CRITERIA MET
1 PRIMARY CRITERION MET
INCIDENT NOT CLASSIFIED AS MAJOR
INCIDENT CLASSIFIED AS MAJOR
CHECK SECONDARY CRITERIA 1 - 'Reputational impact'
CHECK SECONDARY CRITERIA 2 - 'Duration and service downtime'
CHECK SECONDARY CRITERIA 3 - 'Geographical spread'
CHECK SECONDARY CRITERIA 4 – 'Economic impact'
NONE OR ONE SECONDARY CRITERION MET
INCIDENT NOT CLASSIFIED AS MAJOR
2 OR MORE SECONDARY CRITERIA MET
INCIDENT CLASSIFIED AS MAJOR

Simplification of ICT incident classification model

NEW


INCIDENT DETECTION
CHECK CRITERION 'Critical services affected'
CRITICAL SERVICES AFFECTED CRITERION NOT MET
INCIDENT NOT CLASSIFIED AS MAJOR
ANY SUCCESSFUL MALICIOUS UNAUTHORISED ACCESS TO NETWORK AND INFORMATION SYSTEMS
INCIDENT CLASSIFIED AS MAJOR
ASSESSMENT OF OTHER CLASSIFICAITON CRITERIA
CHECK CRITERION 1 'Clients, financial counterparts and transactions'
CHECK CRITERION 2 'Data loss'
CHECK CRITERION 3 'Reputational impact'
CHECK CRITERION 4 'Duration and service downtime'
CHECK CRITERION 5 'Geographical spread'
CHECK CRITERION 6 'Economic impact'
NONE OR ONE ADDITIONAL CRITERION MET
INCIDENT NOT CLASSIFIED AS MAJOR
2 OR MORE ADDITIONAL CRITERIA MET
INCIDENT CLASSIFIED AS MAJOR

Clarification of the definitions (1/3)



A **“Clients affected” now also include:**

- Clients cover also third parties explicitly covered by the contractual agreement between the financial entity and the client as beneficiaries of the affected service
- The impacted clients are those that are or were unable to make use of the service (partially or fully) provided by the financial entity during the incident or that were otherwise adversely impacted by the incident
- The absolute threshold for affected clients should be raised from 50,000 to 100,000 clients

B **Financial counterparts affected**

- The ESAs have decided to increase the relative threshold to 30%, due to potential lead to overreporting and be particularly burdensome for smaller entities as a 10% initial threshold would activate the criterion too soon.

Clarification of the definitions (2/3)

C

Transactions affected:

- Amendment of the requirement in Article 9(1)(d) and (e) of the draft RTS so that it refers to ‘daily average’ number/amount of transactions, instead of ‘regular level of transactions carried out. As a regular level is a hard number to pinpoint
- on the use of different currencies, the ECB’s daily reference exchange rate can be used to come to EUR
- The absolute threshold, has been amended to a relative one with a threshold of 10% of transactions affected.

D

Duration and service downtime

- Amendment of Article 3(2) of the draft RTS by including a reference to unavailability of the service to internal and external users, to further contextualize downtime
- The duration should be measured from the occurrence of the incident and where the occurrence is not known – from the detection of the incident.
- Where the incident has occurred prior to the detection of the incident, FEs shall measure the duration from the records in network or system logs, but that in case they are unable to do so, FEs can apply estimates

Clarification of the definitions (3/3)

E

Data losses:

- Criterion of data loss should be triggered as soon as there is a successful malicious and unauthorised access, irrespective of whether the data has been exploited or not.
- Amendment of Article 5(2) of the draft RTS related to 'authenticity' by focusing on the need to determine whether the incident has compromised the trustworthiness of the source of data

F

Critical services affected changed as follows (article 6):

- Introduced a reference to 'network and information systems' to align better with the incident and major incident-related definitions of DORA;
- Clarified that the authorised services are 'financial services that require authorisation'; and
- Clarify that a successful, malicious and unauthorised access to the network and information systems triggers the criterion of "critical services affected

03

Batch 2 of DORA RTS/ITS - Overview

Thomas Meyer

Batch 2 of DORA RTS/ITS – Overview

Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art.11.1)

RTS to specify the reporting of major ICT-related incidents (Art. 20.a)

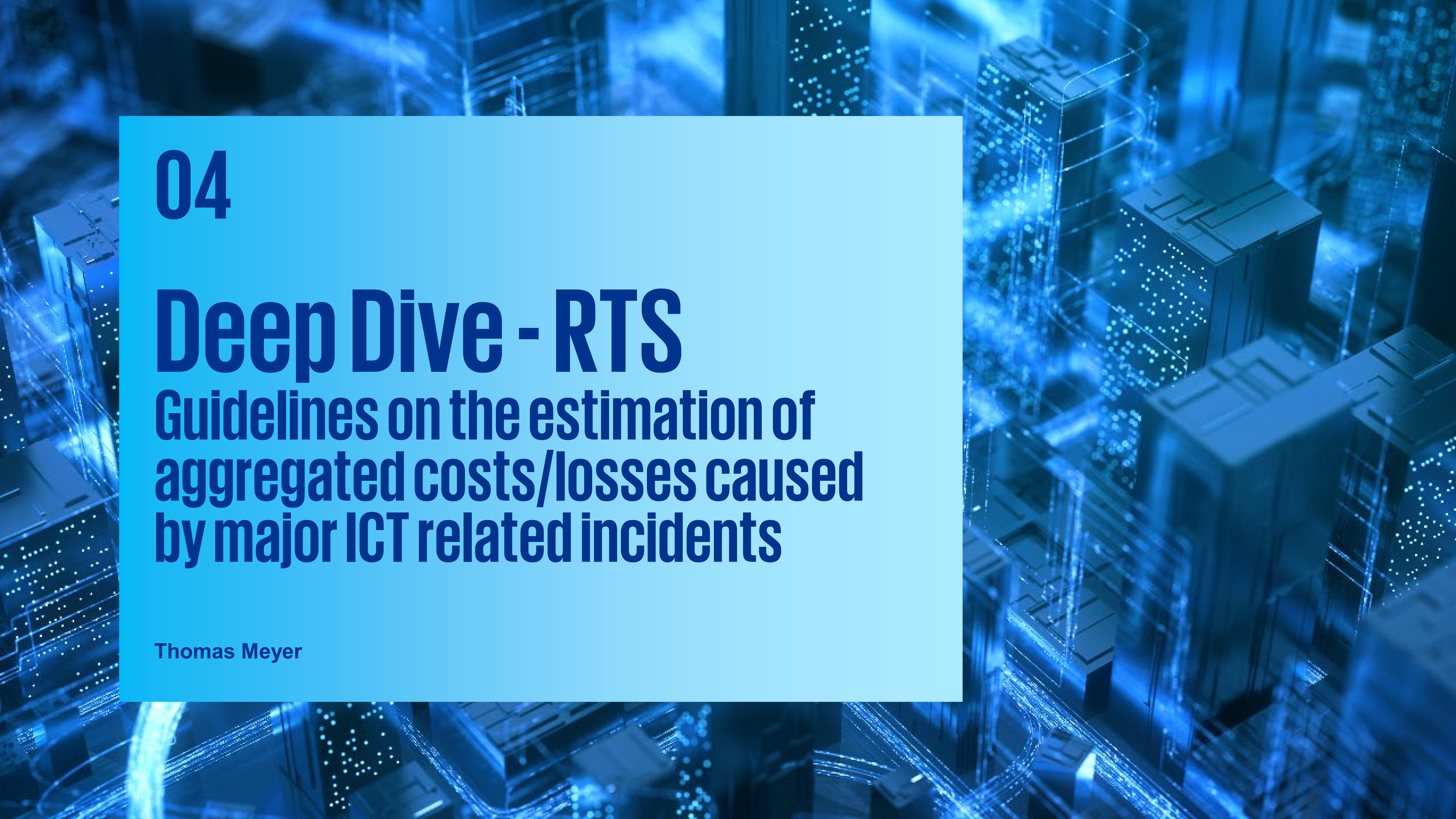
ITS to establish the reporting details for major ICT related incidents (Art. 20.b)

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

RTS specifying criteria for subcontracting ICT services supporting critical or important functions (Art. 30.5)

Guidelines on cooperation ESAs – CAs (Competent Authorities) regarding DORA oversight (Art. 32.7)

RTS on harmonisation of oversight conditions (Art. 41)



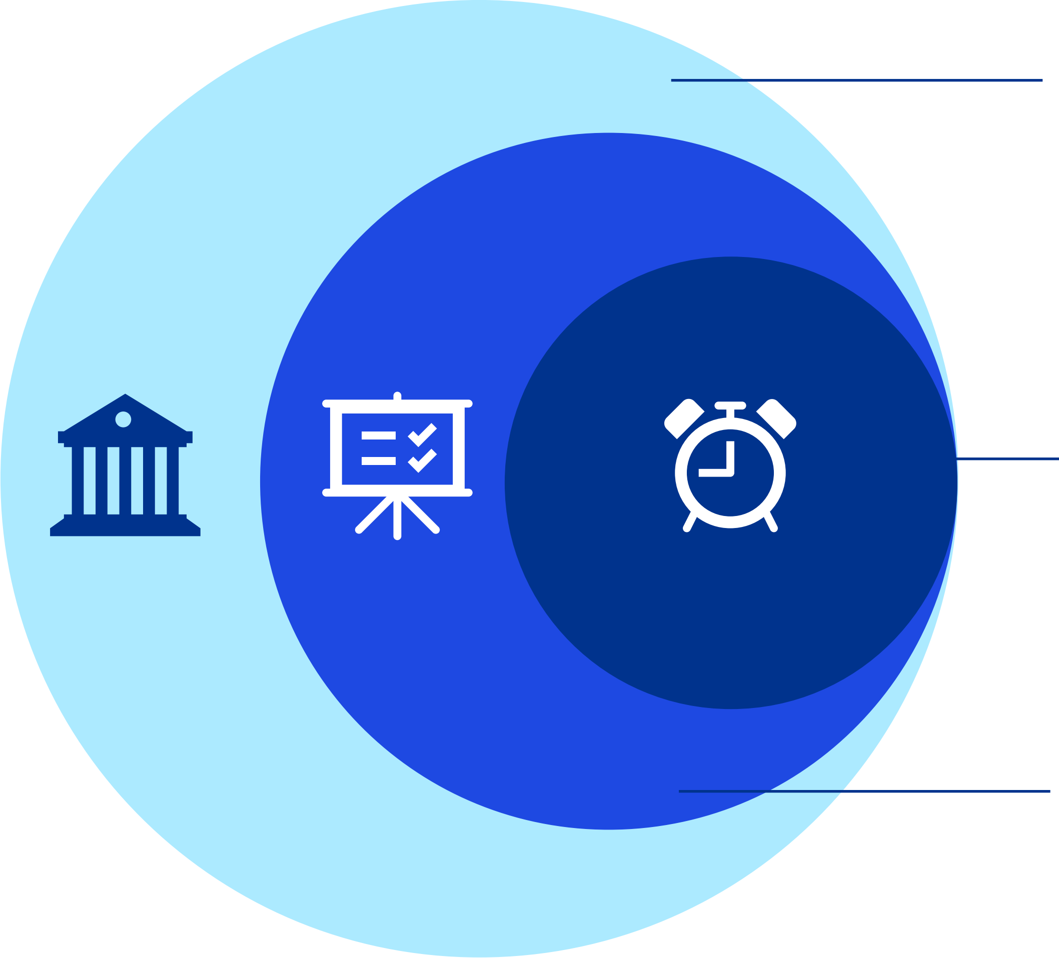
04

Deep Dive - RTS

Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents

Thomas Meyer

Summary



Mandate Overview

- **Article 11(11)** of DORA mandates ESAs to develop common guidelines on estimating **aggregated annual costs and losses from major ICT-related incidents**
- Aim is to harmonize estimation practices by financial entities for reporting to competent authorities (CAs)

Consultation Period

- Consultation paper open until 4 March 2024
- Final guidelines to be published post-consultation period (Target date for the proposal to the EU Commission: July 24)

Objectives

- Guidelines aim to harmonize how financial entities estimate aggregated annual costs and losses for major ICT-related incidents
- Enable CAs to utilize aggregated costs and losses for assessing the effectiveness of ICT risk management frameworks in financial entities
- Contribution to a risk-based approach and increased efficiency in supervision

Provisions on the estimation of aggregated annual costs and losses of major ICT-related incidents

Estimation Scope

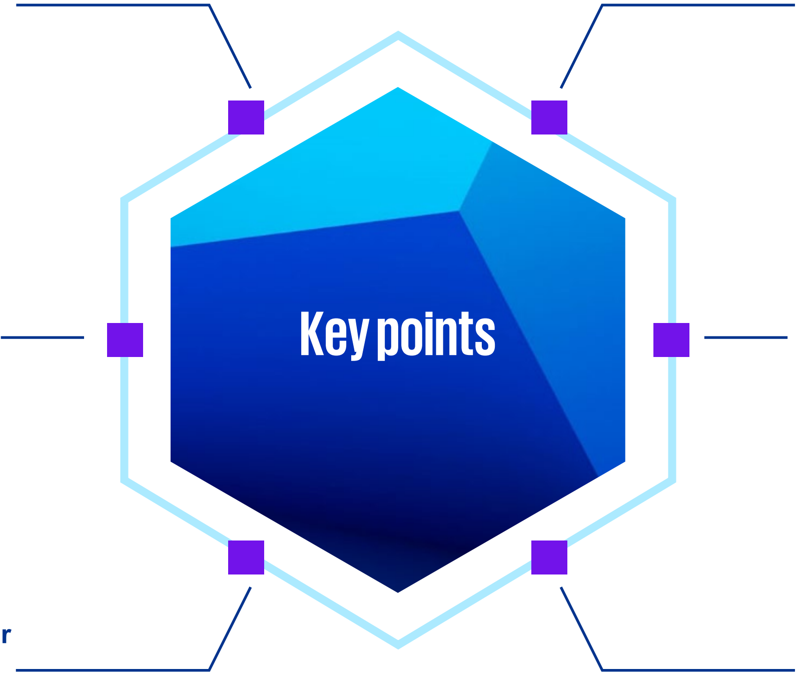
- Financial entities should **estimate** aggregated annual costs and losses for major ICT-related incidents **within the reference period** requested by the competent authority
- Costs and losses related to incidents **before or after the reference period** should be **excluded**

Estimation Basis

- Refer to costs, losses, and financial recoveries in financial statements, **validated by an independent entity**
- Include **accounting provisions** from validated financial statements

Inclusion Criteria

- **Include all ICT-related incidents classified as major** according to the RTS on incident classification.
- Include incidents - for which a final report was submitted in the relevant accounting year or in previous years **that had a quantifiable financial impact**



Sequential Estimation

- Estimate gross costs and losses **for each major ICT-related incident based on types** specified in the RTS on incident classification
- **Calculate** net costs and losses for each incident **by deducting financial recoveries**
- **Aggregate** gross costs and losses, financial recoveries, and net costs and losses **across major ICT-related incidents**

Notification & Compliance

- Competent authorities must notify the respective ESA regarding compliance with the guidelines within two months of issuance

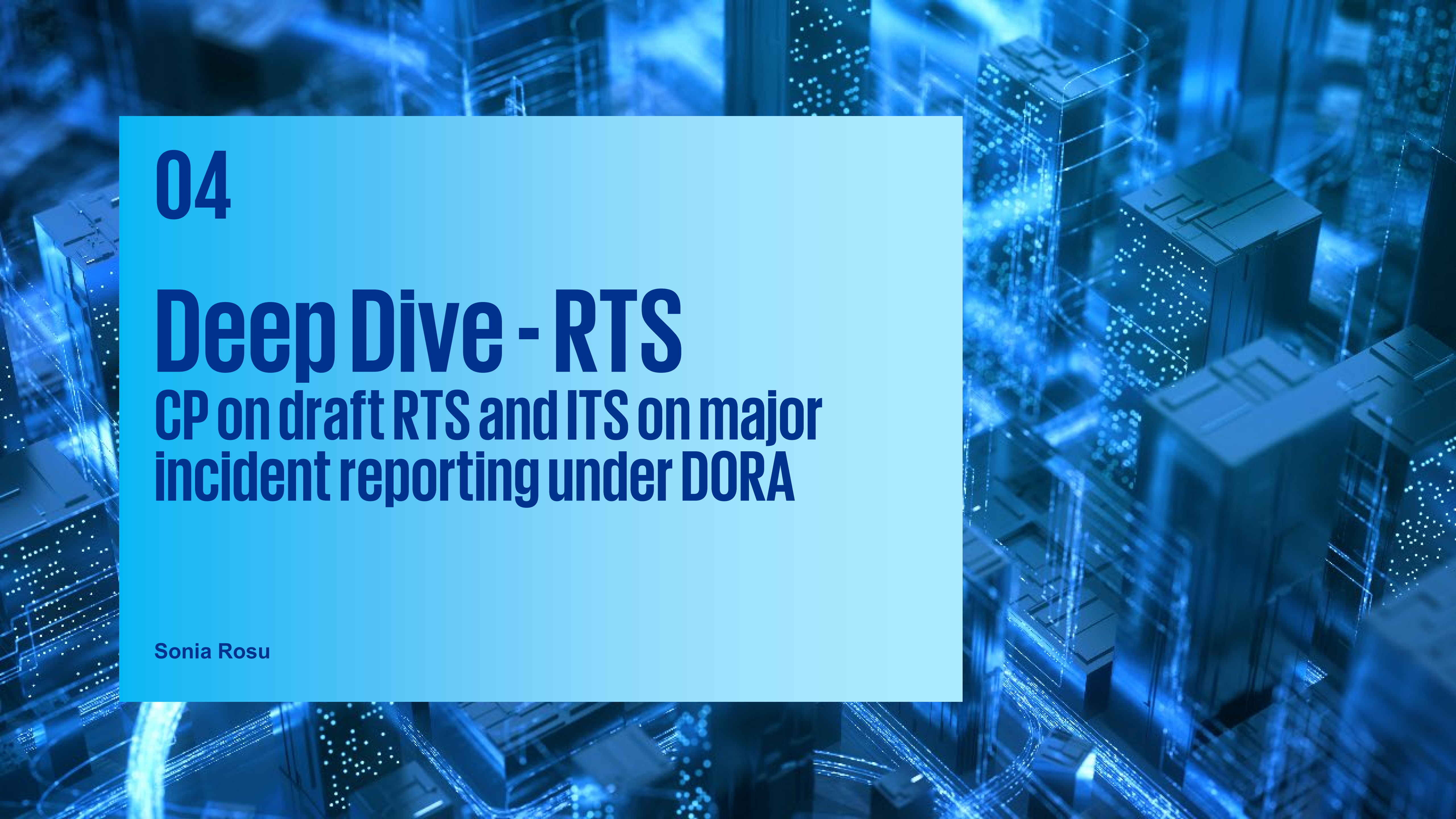
Adjustments & Reporting

- **Include adjustments** for costs and losses **reported in the previous year's** aggregated reporting
- **Breakdown gross and net costs and losses** for each major ICT-related incident in the report
- Use the **provided template** in the Annex for reporting

Reporting template for gross and net costs and losses in an accounting year

Name of the financial entity	
Start and end date of accounting year of the financial entity	
Reporting currency	

Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the accounting year	Recoveries of the incident in the accounting year	Net costs and losses of the incident in the account year
1					
2					
…					
Aggregated annual costs and losses	-----------	-----------			



04

Deep Dive - RTS

CP on draft RTS and ITS on major incident reporting under DORA

Sonia Rosu

Summary of RTS and ITS content for ICT incident reporting

JC 2023 70 - CP on draft RTS and ITS on major incident reporting under DORA.docx (europa.eu)

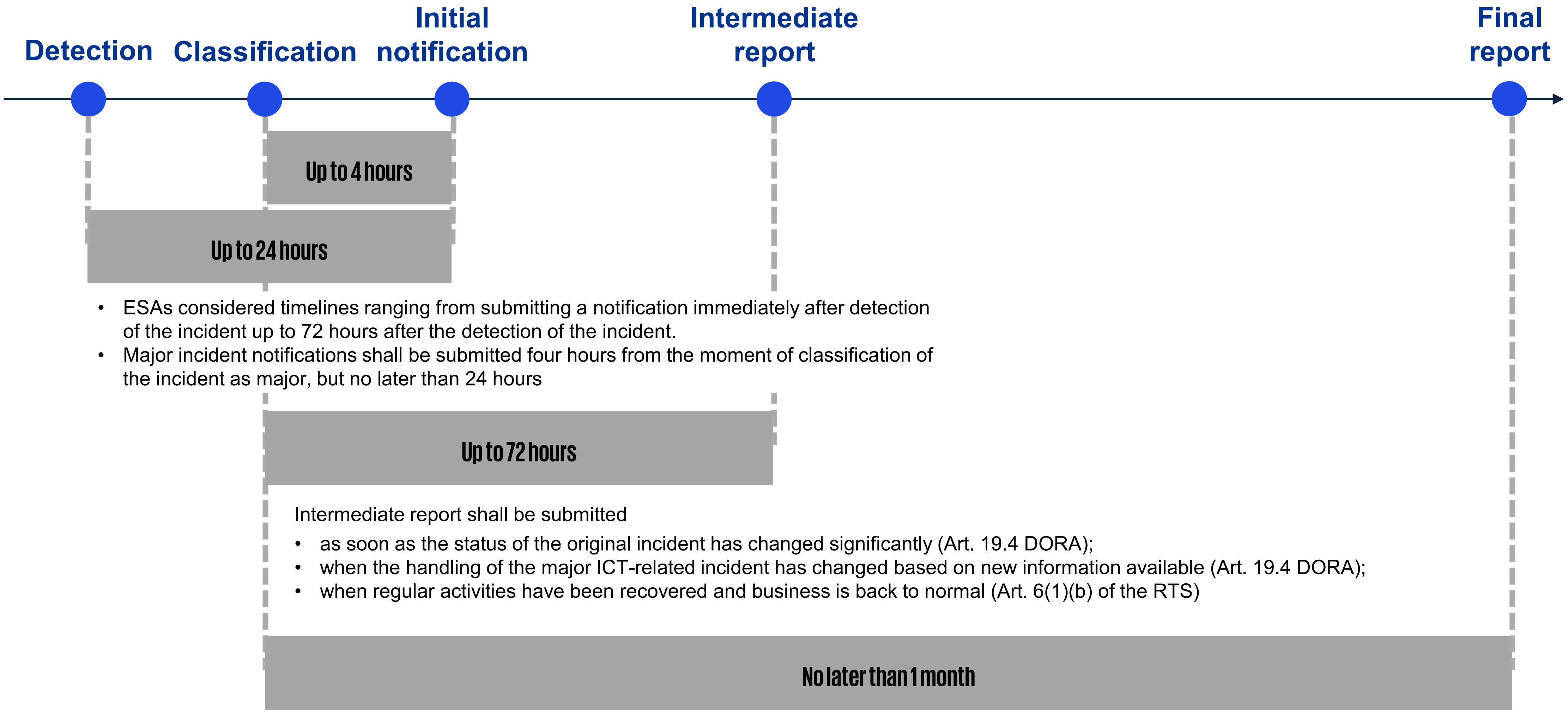
Regulatory Technical Standards (RTS) establishing the content of the reports for ICT related incidents and the notification for significant cyber threats, and the time limits to report incidents.

- The initial notification up to 4 hours from the classification of the incident by the FE as major, but no later than 24 hours from the detection of the incident.
- Submission of the intermediate report is 3 days (72 hours) after the classification of the incident as major, or when regular status has resumed.
- In relation to the final report, which will require additional level of detail to the intermediate report, including root cause analysis and information about the actions taken, the ESAs expect to be submitted within 1 month from the classification of the incident as major, unless it has not been resolved – when it has been resolved it must be submitted the next day.

Implementing Technical Standards (ITS) establishing the standard forms, templates and procedures to report a major ICT-related incident or to notify a significant cyber threat.

- Reporting template cover 37 specific types of data, spread between
  - general information about the reporting FE
  - initial notification
  - intermediate report and
  - final report

Reporting timeline for major ICT incidents



Detection

Classification

Initial notification

Intermediate report

Final report

Up to 4 hours

Up to 24 hours

- ESAs considered timelines ranging from submitting a notification immediately after detection of the incident up to 72 hours after the detection of the incident.
- Major incident notifications shall be submitted four hours from the moment of classification of the incident as major, but no later than 24 hours

Up to 72 hours

Intermediate report shall be submitted

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

No later than 1 month

General FE information

General information is mandatory for all reporting phases.

Content described in Annex II.

24h

General financial entity information contains :

- Type of report, name, type and LEI code of the reporting and/or affected financial entity, identification of the parent undertaking
- Contact details of responsible persons within the affected financial entity or a third-party reporting on behalf of the affected financial entity;
- Reporting currency

18	Data rows in total
4	Choice datapoints
14	Alphanumeric datapoints
3	Number datapoints
0	Date or time datapoints

KPMG

Initial notification

Initial notification is focusing on early information sharing.

Content described in Annex II.

24h

Initial notification contains :

- **Date and time** of detection and classification of the incident
- **Description** of the incident
- Classification **criteria** that triggered or are likely **to trigger** the incident report
- Members States impacted or potentially impacted by the incident
- Information about the origin of the incident
- **Indication on the impact** or potential impact on other financial entities and/or third-party providers
- Information whether the incident is **recurring or relates to a previous incident**
- Indication of **activation of business continuity plan**

16

Data rows in total

7

Choice/Boolean datapoints

6

Alphanumeric datapoints

1

Number/Integer datapoints

2

Date or time datapoints

Intermediate report

Intermediate report is focusing on recovery actions and possible impact to other entities.

Content described in Annex II.

72h

Intermediate report contains :

- Incident reference code, incident type, classification criteria and Information on how the incident has been discovered
- Indication whether the **incident originates** from a third-party provider or other financial entity
- Date and time of occurrence of the incident and **when regular activities have been recovered** and business is back to normal
- **Temporary actions taken** or planned to be taken to recover from the incident
- Information on the impact on other financial entities, **affected functional areas and business processes**, affected infrastructure components
- **Indication on communication** to stakeholders, Information about reporting to law enforcement
- Information on **vulnerabilities exploited** and indicators of compromise

41	Data rows in total
13	Choice/Boolean datapoints
16	Alphanumeric datapoints
7	Number/Integer/monetary/percentage datapoints
5	Date or time datapoints

Final report

Final report is focusing on impact and financial calculations, cost and losses.

Content described in Annex II.

Final report contains:

- Information about the **root cause of the incident**, inability to comply with legal requirements and breach of contractual arrangements/SLAs
- Date and time **when the incident was resolved** and the root cause addressed
- Information on the **measures and actions taken** for the resolution of the incident and **additional controls** to prevent similar incidents in the future
- Information about the **reclassification** of a major incident to non-major, Information relevant for resolution authorities
- Information about **direct and indirect costs and losses** stemming from the incident and information about financial recoveries

25
Data rows in total

3
Choice/Boolean datapoints

10
Alphanumeric datapoints

11
Number/integer/monetary/ percentage datapoints

1
Date or time datapoints

Cyber threat reporting

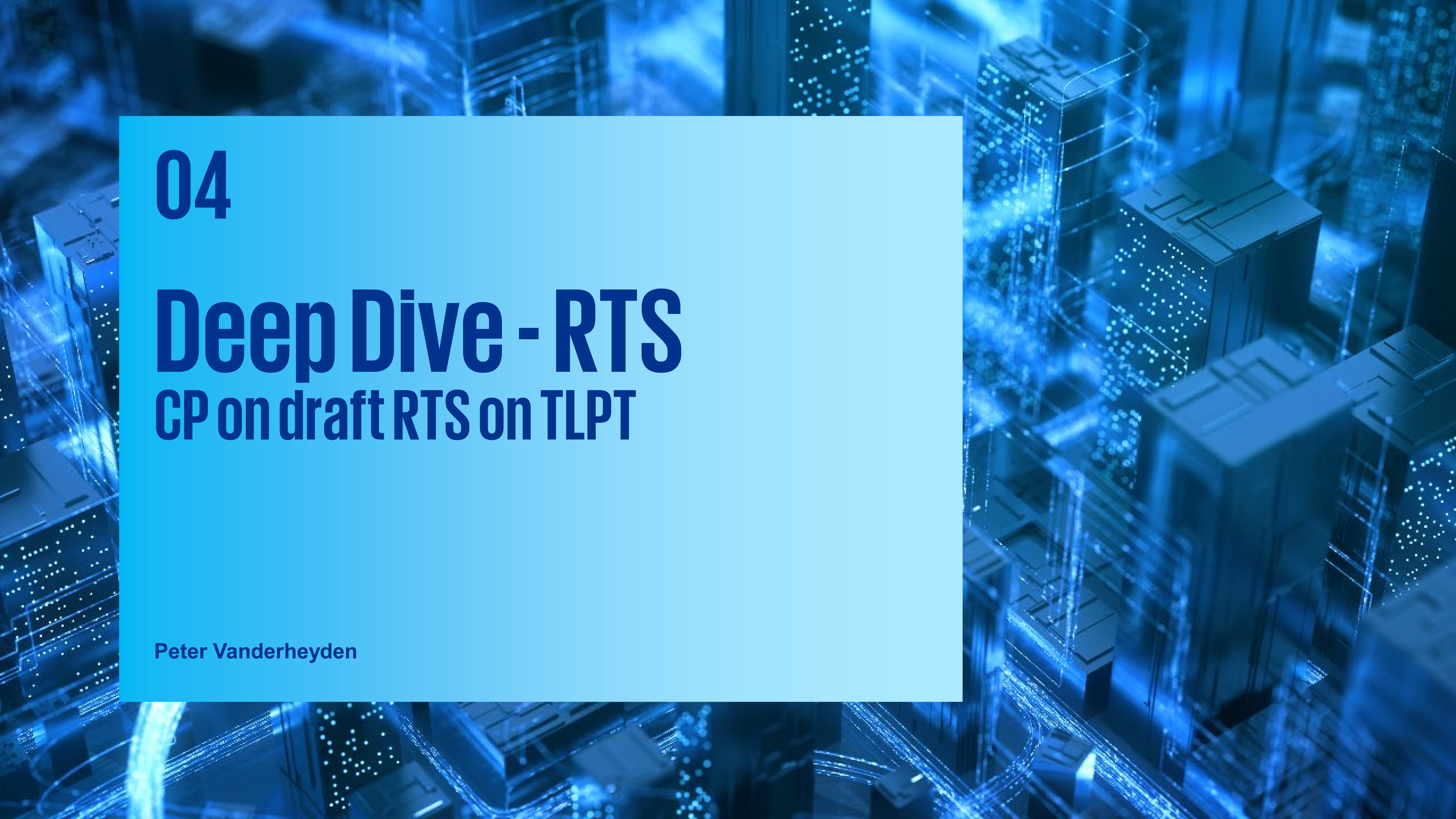
Cyber threat notification is voluntary.

Content is described in Annex IV

Cyber threat notification

- Date and time of detection of the cyber threat
- Description of the significant cyber threat, date and time for detection, incident classification criteria
- Information about potential impact, status of prevention, indicators of compromise
- Notification to other stakeholders

21	Data rows in total
4	Choice datapoints
14	Alphanumeric datapoints
2	Number datapoints
1	Date or time datapoints



04

Deep Dive - RTS

CP on draft RTS on TLPT

Peter Vanderheyden

Summary of Threat-Led Penetration Testing (TLPT)

The goal of TLPT is to evaluate the effectiveness of implemented security controls against advanced cyber threats

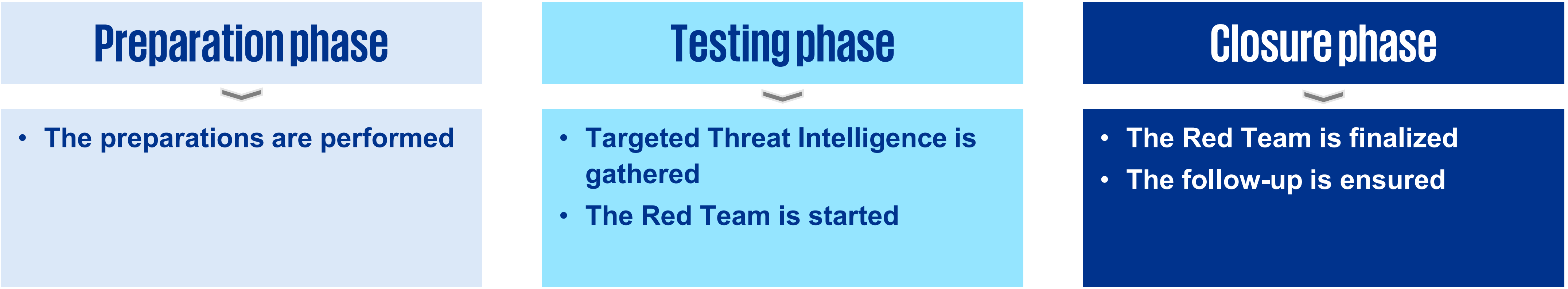
TLPT must be performed at least partly by an external provider and at least once every three years

The scope of TLPT includes the production systems, including critical and important functions and even ICT 3rd parties

A summary of relevant findings and remediation plans are submitted to the governing authority

Phases overview of TLPT

TLPT’s RTS follows the Threat Intelligence Based Ethical Red Teaming (TIBER-EU) framework



Preparation phase

- The preparations are performed

Testing phase

- Targeted Threat Intelligence is gathered
- The Red Team is started

Closure phase

- The Red Team is finalized
- The follow-up is ensured

Preparation phase

Preparation phase

The preparations are performed:

- The documentation and templates are shared by the TLPT Authority
- The Threat Intelligence Provider (TIP) and Red Teaming Provider (RTP) are procured
    - Red Teaming can be done by internal pentesters every 2 out of 3 TLPT
- The goals and expectations are aligned during a launch meeting
- A Control Team is formed to guide the test
- The scoping is discussed and finalized with the Control Team (CT), the TLPT Authority, and the RTP and TIP
- A final meeting is organized to create board level engagement

Deliverables:

- Procured TIP and RTP
- Test Scoping document
- Project planning
- Board level engagement

Testing phase

Testing phase

Targeted Threat Intelligence is gathered:

- The Threat Intelligence Provider (TIP) gathers threat intelligence in a passively manner based on the scoping document
- The TIP provides the Threat Intelligence Report

The Red Team is started:

- The Red Teaming Provider (RTP) provides Test Scenarios based on the TI Report
- The CT together with the RTP and the TLPT Authority chooses relevant scenarios (minimum 3)
- The RTP provides a Test Plan based on the selected scenarios
- The RTP performs the Red Team over a minimum of 12 weeks

Deliverables:

- Threat Intelligence Report
- Test Scenarios and Test Plan
- Red Team test

Closure phase

Closure phase

The Red Team is finalized:

- The RTP provides the Red Team Report
- The Blue Team (BT) provides their Blue Team Report
- The RT and BT together hold a Purple Teaming

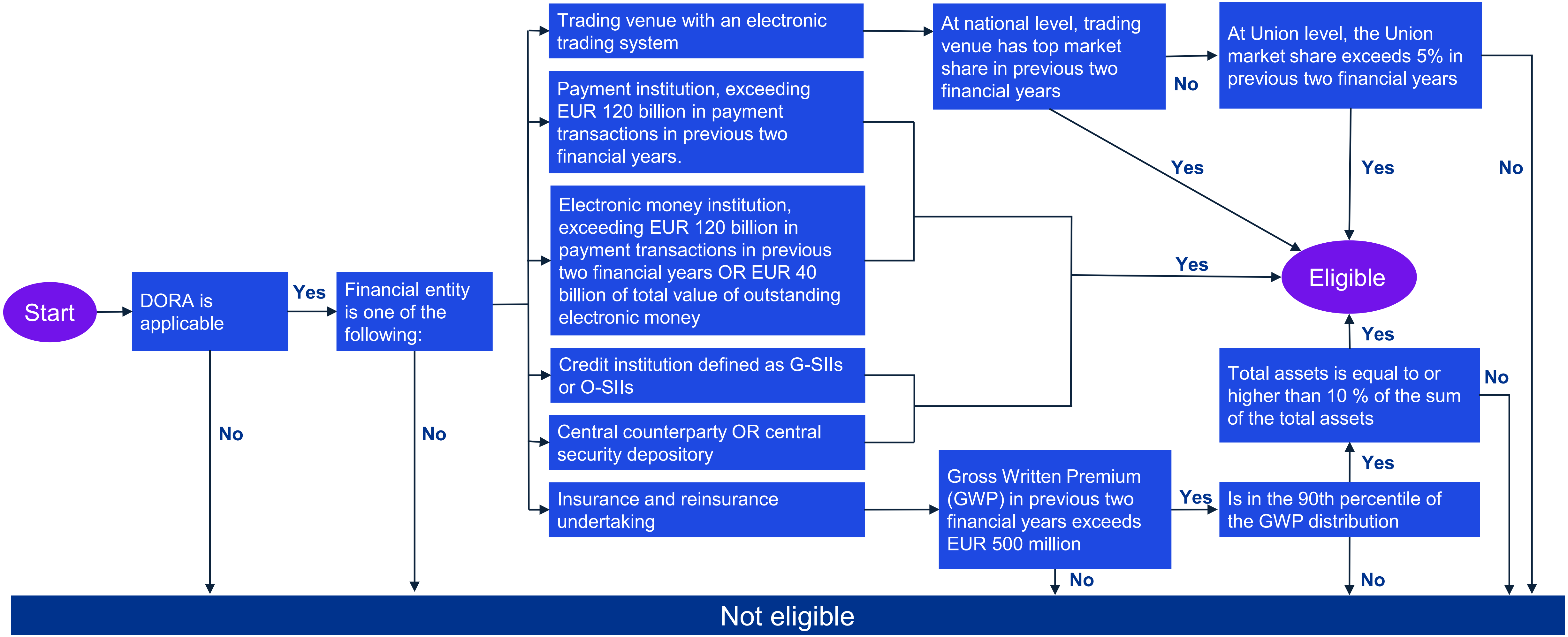
The follow-up is ensured:

- The Financial Entity creates a Remediation plan and provides the Test Summary to the TLPT Authority

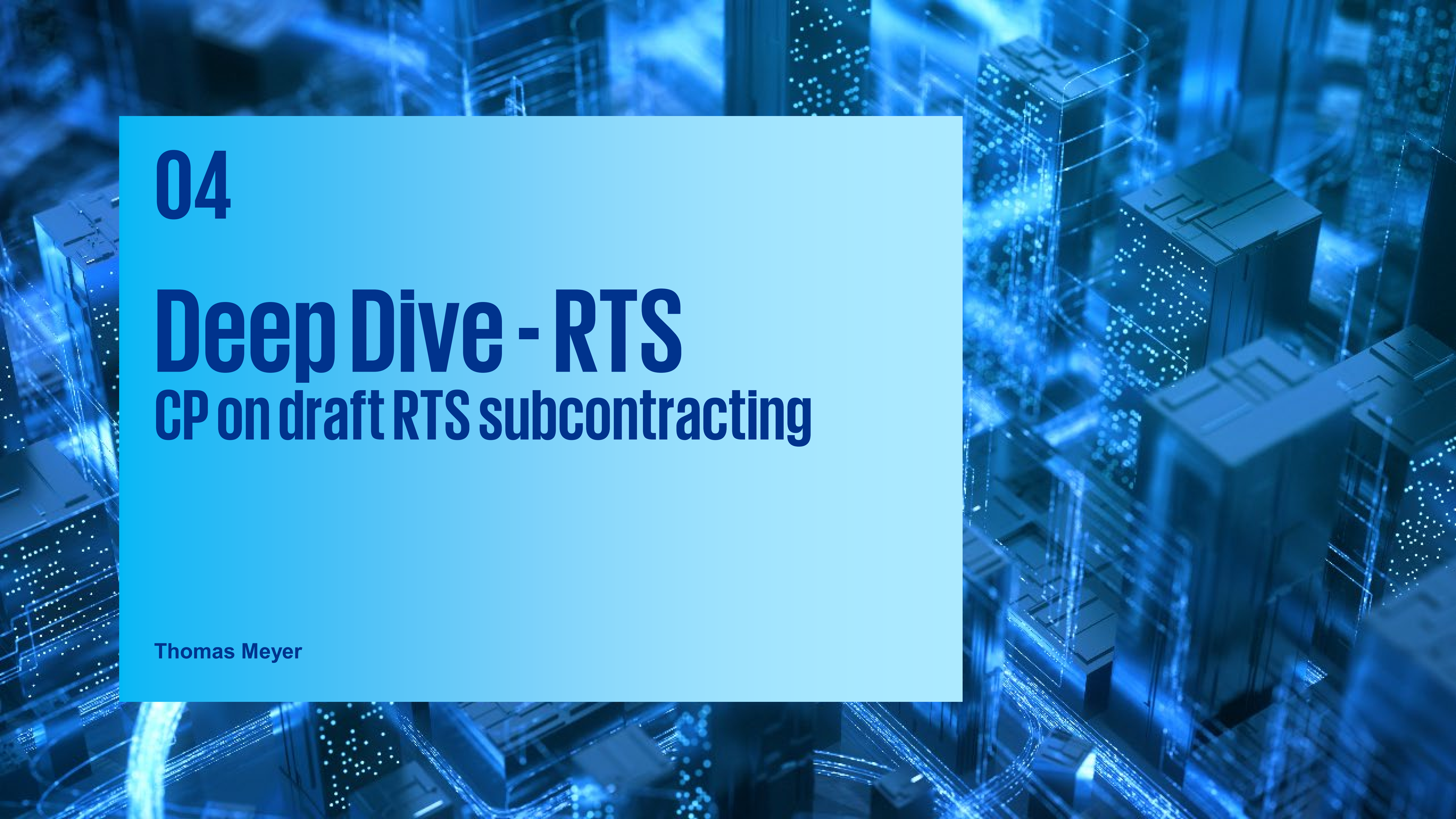
Deliverables:

- Red Team Report
- Blue Team Report
- Purple Teaming session(s)
- Remediation Plan
- Test Summary

Eligibility of TLPT



Start
DORA is applicable
Yes
Financial entity is one of the following:
Trading venue with an electronic trading system
Payment institution, exceeding EUR 120 billion in payment transactions in previous two financial years.
Electronic money institution, exceeding EUR 120 billion in payment transactions in previous two financial years OR EUR 40 billion of total value of outstanding electronic money
Credit institution defined as G-SIIs or O-SIIs
Central counterparty OR central security depository
Insurance and reinsurance undertaking
At national level, trading venue has top market share in previous two financial years
No
At Union level, the Union market share exceeds 5% in previous two financial years
Yes
Yes
No
Yes
Eligible
Yes
Total assets is equal to or higher than 10 % of the sum of the total assets
No
Yes
Gross Written Premium (GWP) in previous two financial years exceeds EUR 500 million
Yes
Is in the 90th percentile of the GWP distribution
No
No
No
No
Not eligible



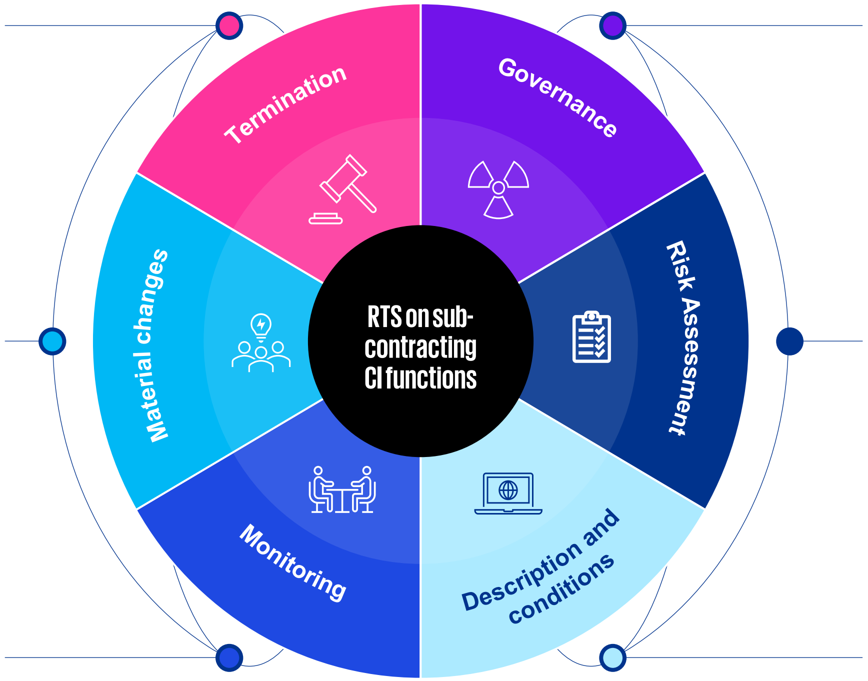
04

Deep Dive - RTS

CP on draft RTS subcontracting

Thomas Meyer

The RTS on subcontracting CI functions follows the contractual lifecycle



Termination of the contractual arrangement (Art. 7)

- Material changes despite the objection
- Subcontracting without permission

Material changes to subcontracting arrangements (Art. 6)

- Information with a sufficient advance notice period
- Implementation only after approval or no objection
- Modification right based on the risk exposure

Monitoring of the entire ICT subcontracting chain by the FE (Art. 5)

- Basis is the register of information
- Monitoring of the subcontracting conditions

- **Proportionality (Art. 1)**
- **Group application (Art. 2)**

Risk assessment regarding the use of subcontractors (Art. 3)

- Decision on subcontracting only after risk assessment
- Periodic assessment of changes in the business environment and assessment of ICT, concentration and geopolitical risks

Description and conditions under which the ICT services supporting CI functions may be subcontracted (Art. 4)

- Identification of ICT services eligible for subcontracting and description of conditions
- Specification of the written contractual agreement

The risk assessment on the use of subcontractors

Decision to subcontract (Art.3 (1))

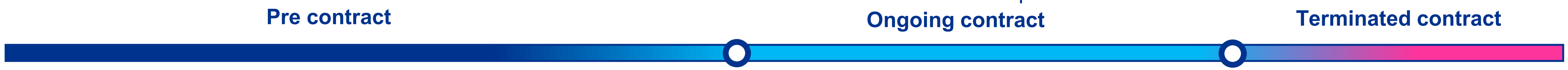
Only after having assessed at least:

- the appropriateness of the due diligence processes of the ICT TPP regarding subcontracting
- the abilities of the ICT TPP to inform and involve the FE in the decision-making of subcontracting
- that relevant contractual clauses are replicated in the subcontracting arrangements
- the adequacy of the abilities and governance structures of the ICT TPP to monitor subcontractors
- that the FE has abilities and governance structures to monitor subcontracted ICT services or subcontractors
- the impact of a possible failure of a subcontractor
- the risks associated with the geographical location of the potential subcontractors
- the ICT concentration risks
- any obstacles to the exercise of audit, information and access rights

Periodic assessment (Art.3 (2))

FEs shall periodically carry out the assessment of:

- Risks based on possible changes in the business environment, including but not limited to changes in the supported business functions
- ICT, concentration and geopolitical risks



Contractual agreements for subcontracting

FEs shall identify which ICT services support CI functions and which of those are eligible for subcontracting and under which conditions. For each ICT service eligible for subcontracting the written contractual agreement shall specify:

Monitoring requirements for the ICT TPP regarding subcontracting to ensure contractual obligations with the FE (Art. 4 a))

Monitoring and reporting obligations of the ICT TPP towards the FE (Art. 4 b))

Requirements for the ICT TPP regarding the assessment of risks, including ICT risks, associated with the location of the potential subcontractor and the provision of ICT services (Art. 4 c))

The location and ownership of data processed or stored by the subcontractor, where relevant (Art. 4 d))

Specification requirements for the ICT TPP regarding the monitoring and reporting obligations of the subcontractor (Art. 4 e))

Requirements for the ICT TPP to ensure the continuous provision of the ICT services, even in case of failure by a subcontractor to meet service levels or any other contractual obligations (Art. 4 f))

Compliance requirements of incident response and business continuity plans and service levels of ICT subcontractors (Art. 4 g))

Compliance requirements for ICT security standards and any additional security features, where relevant, to be met by the subcontractors (Art. 4 h))

Requirements for the subcontractor to grant to FEs and CAs the same audit, information and access rights as granted by the ICT TPP (Art. 4 i))

Appropriate termination rights for the FE (Art. 4 j))

05

DORA & Operational Risk

Kris Vancolen

The Bigger picture: resilience & nonfinancial risk management

Operational Resilience is a key focus area for the regulator.

However, resilience is not just something you will do because the regulator asks you so. You want to be resilient because you need to be able to achieve your companies' objectives in a competitive and (sometimes) hostile world.

Operational Resilience, when done properly, will be also the result of good Operational Risk Management. In other words, the more robust your Operational Risk Management framework is - you can see it as your foundational work - the better your chances are to have an effective DORA implementation.

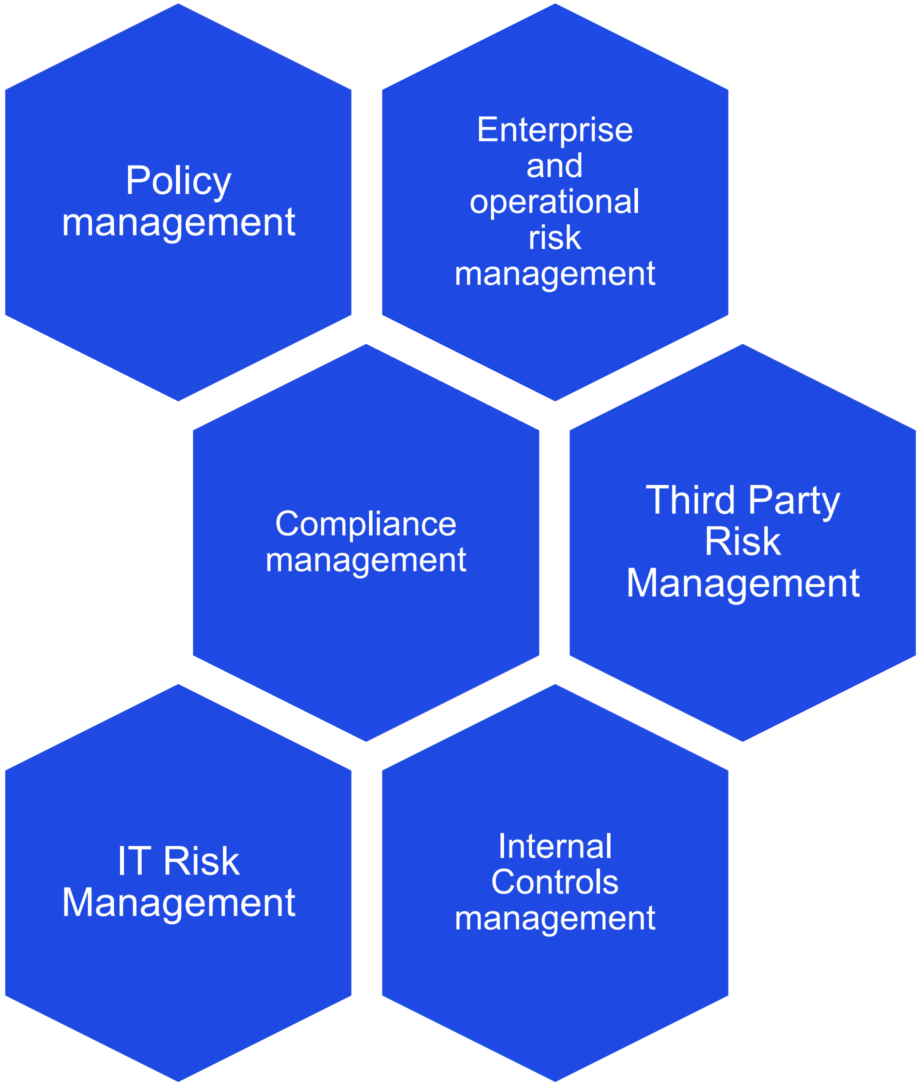
While running a **DORA-related project**, you might detect areas in your risk management framework that are perhaps not as mature as you would wish them to be.

Examples could be

- the organization of your 3 lines of defense with unclear responsibilities and redundant controls, or
- The way your third-party risk management is run, might not be optimal or mature
- You might lack the resources or have silos between stakeholder departments
- Your culture of controls where perhaps people hesitate to raise their hand when they see an issue
- Segmented tooling

The idea would that you also think about your target operating model for the management of nonfinancial risks, including when it comes to cyber resilience. You can for example perform a capability maturity assessment of the foundational aspects of your risk management framework.

So, while focusing on DORA, do not forget the foundations



Policy management

Enterprise and operational risk management

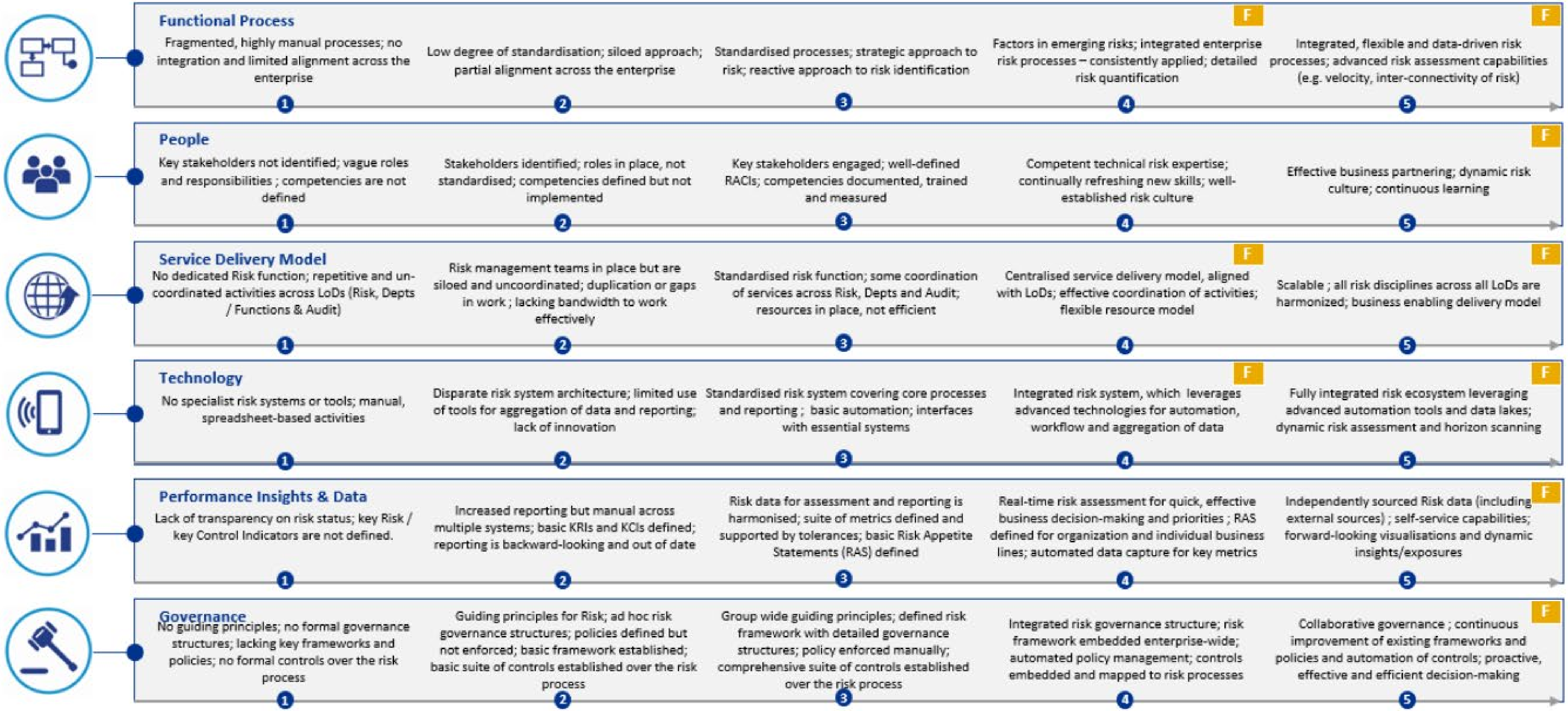
Compliance management

Third Party Risk Management

IT Risk Management

Internal Controls management

The Bigger picture: example of a maturity model



	1	2	3	4	5
Functional Process	Fragmented, highly manual processes; no integration and limited alignment across the enterprise	Low degree of standardisation; siloed approach; partial alignment across the enterprise	Standardised processes; strategic approach to risk; reactive approach to risk identification	F Factors in emerging risks; integrated enterprise risk processes – consistently applied; detailed risk quantification	F Integrated, flexible and data-driven risk processes; advanced risk assessment capabilities (e.g. velocity, inter-connectivity of risk)
People	Key stakeholders not identified; vague roles and responsibilities ; competencies are not defined	Stakeholders identified; roles in place, not standardised; competencies defined but not implemented	Key stakeholders engaged; well-defined RACIs; competencies documented, trained and measured	Competent technical risk expertise; continually refreshing new skills; well-established risk culture	F Effective business partnering; dynamic risk culture; continuous learning
Service Delivery Model	No dedicated Risk function; repetitive and un-coordinated activities across LoDs (Risk, Depts / Functions & Audit)	Risk management teams in place but are siloed and uncoordinated; duplication or gaps in work ; lacking bandwidth to work effectively	Standardised risk function; some coordination of services across Risk, Depts and Audit; resources in place, not efficient	F Centralised service delivery model, aligned with LoDs; effective coordination of activities; flexible resource model	F Scalable ; all risk disciplines across all LoDs are harmonized; business enabling delivery model
Technology	No specialist risk systems or tools; manual, spreadsheet-based activities	Disparate risk system architecture; limited use of tools for aggregation of data and reporting; lack of innovation	Standardised risk system covering core processes and reporting ; basic automation; interfaces with essential systems	F Integrated risk system, which leverages advanced technologies for automation, workflow and aggregation of data	F Fully integrated risk ecosystem leveraging advanced automation tools and data lakes; dynamic risk assessment and horizon scanning
Performance Insights & Data	Lack of transparency on risk status; key Risk / key Control Indicators are not defined.	Increased reporting but manual across multiple systems; basic KRIs and KCIs defined; reporting is backward-looking and out of date	Risk data for assessment and reporting is harmonised; suite of metrics defined and supported by tolerances; basic Risk Appetite Statements (RAS) defined	Real-time risk assessment for quick, effective business decision-making and priorities ; RAS defined for organization and individual business lines; automated data capture for key metrics	F Independently sourced Risk data (including external sources) ; self-service capabilities; forward-looking visualisations and dynamic insights/exposures
Governance	No guiding principles; no formal governance structures; lacking key frameworks and policies; no formal controls over the risk process	Guiding principles for Risk; ad hoc risk governance structures; policies defined but not enforced; basic framework established; basic suite of controls established over the risk process	Group wide guiding principles; defined risk framework with detailed governance structures; policy enforced manually; comprehensive suite of controls established over the risk process	Integrated risk governance structure; risk framework embedded enterprise-wide; automated policy management; controls embedded and mapped to risk processes	F Collaborative governance ; continuous improvement of existing frameworks and policies and automation of controls; proactive, effective and efficient decision-making

05

Q&A

Q&A – General (1/2)

What are the most common challenges for banks and insurance companies when implementing the DORA requirements?

There are multiple regulatory requirements to fulfill within the same timeline (i.e., CSRD, IFRS17) resulting in a lot of work.

- Starting too late with assessing the impact of DORA and consequently implementing it
- Lack of knowledge and resources to follow up on DORA

Specific DORA points:

- Not starting contract negotiations with ICT third parties for DORA requirements
- Not incorporating the draft RTS/ITS in the gap assessments and waiting for the final drafts

How does DORA affect the current IT infrastructure and what changes are required to comply with the new regulations?

When we look at the impact on the IT infrastructure, we mainly see an impact in relation to the management of the IT infrastructure.

From that point of view, it comes down the following categories:

- Overall update to IT governance processes
- Framework changes from an ICT risk management
- Changes to underlying processes, policies and procedures (RTS ICT Risk, Incident, TPRM), some requiring a lot of detail

Lastly, it's about having proper and detailed insight into your IT Infrastructure and internal links, so you are able to determine the impact on the whole infrastructure if one component fails.

Can you provide best practices for establishing a robust ICT risk management framework in line with DORA's guidelines?

Yes, we can help with that. Please contact us.

How does DORA suggest financial institutions manage and mitigate ICT risk?

Through an improved management cycle which is adapted to the increased complexity internally and externally.

Q&A – General (2/2)

How should banks and insurance companies approach the auditing process to ensure compliance with DORA?

You should ensure that you have knowledgeable and experienced people checking DORA.

Does the IT provider fall under DORA if it is situated in Switzerland?

It does. The main party receiving services from the Swiss provider should demonstrate that the main party in the outsourcing chain, which includes the Swiss provider, is DORA compliant.

You discussed an update to security and awareness training and mentioned that it has been "scrapped/deleted". Does this mean that the requirement to provide security and awareness training has been removed/descoped from DORA?

Yes, it has been outscoped. However, this does not mean that it does not matter, but that you should take care of it yourself as an organization.

Q&A – ICT-related incidents

Is loss of sales (turnover) also part of the incident costs?

Yes, definitely.

Is it correct that the initial notification/final report needs to be submitted within 72 hours from detection and within 24 hours from classification?

Initial notification shall be submitted no later than 24 hours from the time of detection of the incident after the FE has classified the incident as major.

Intermediate report shall be submitted within 72 hours of the classification of the incident as major.

Final report shall be submitted within 1 month.

You mentioned the requirement for third parties to notify the FE's of incidents occurring on their premises, in order for the FE's to have an overall view or register of all ICT-related incidents. Could you please provide further details on how this requirement is linked to the guidelines on costs and losses caused by major ICT-related Incidents? When these two regulations are combined, does it mean that third parties should also provide information on costs, such as resolution costs for incidents? Should FE's take these costs into consideration, regardless of whether they directly impact the financial entity or not?

There is no requirement for ICT third party service providers to report on their costs to their clients, and these costs should not be used or reported by the impacted clients: only the costs incurred by the client have to be taken into account in the report.

Q&A – TLPT (1/3)

What types of tests does DORA require as a minimum?

DORA Article 25 provides the following examples of types of testing, without specifying what is required as a minimum: "The digital operational resilience testing program referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing."

Is there a specific reason why authorities are requiring the use of third-party providers for the Threat Intelligence phase?

Internal testers are only allowed for TLPT in special conditions. We have no additional insight into the reason to mandate external Threat Intelligence Providers, but one of the reasons could be to have an unbiased point of view (free of potential conflict of interest) and a neutral approach to the high-level attack scenarios and relevant threat actors. If you would like to know more about this, or provide an alternative point of view, you can respond to the consultation (JC 2023 72) before 4 March 2024, specifically to questions 6 and 7 of Annex II.

Is it KPMG's advice or a written requirement from the ESA's that an organization should not be aware of TLPT tests in order for them to be meaningful?

It is both a written requirement and the advice of KPMG. The TLPT should be performed, according to the RTS, "in accordance with the TIBER-EU framework". The TIBER-EU framework Chapter 6.5 details the confidentiality of the test: "Protecting the confidentiality of the test is crucial to its effectiveness. To that end, the entity should limit awareness of the test to a small trusted group whose members have the appropriate levels of seniority to make risk-based decisions regarding the test."

Is there any elaboration in the RTS on TLPT regarding which financial entities should perform these tests, or is it mandatory for every financial firm to conduct TLPT?

Yes, please refer to slide 54 of our webinar.

Q&A – TLPT (2/3)

What is the opinion on the proposed requirement in RTS that the red team testing should take a minimum of 12 weeks? Wouldn't it make more sense to limit security and service risk on production systems by not having a minimum duration, if the TLPT objective is achieved?

As part of TLPT, every test should contain at least 3 attack scenarios. To simulate advanced and persistent threat actors, it is necessary that the Red Team has sufficient time to perform the complete cyber attack kill chain. As part of TLPT, a Test Plan is mandatory detailing the cyber attack scenarios and the corresponding timelines. In exceptional circumstances, the Red Team can deviate from these timelines, but in principle should try to meet them, and not go faster. If all three scenarios are completed within the 12 weeks, the tested entity and Red Team can discuss this with the competent authority and if the reasons are valid, it is our view that it seems unlikely that the competent authority will declare the test invalid because of the duration.

Does the TLPT have to be carried out in the production environment?

Yes, TLPT need to be done in production environment and appropriate risk mitigating controls should be in place. E.g., point 35 (page 12) of the RTS states the following: "A key way to minimize risk associated with TLPT is the selection of experienced, suitable and highly skilled testers and TI providers. As testing takes place on live production systems, only experienced providers should be selected."

Q&A – TLPT (3/3)

If an insurance company's gross written premiums exceed 500 million, it must apply the sections on penetration testing in the DORA regulation. Does this 500 million threshold apply at group level or at individual company level?

The complete rules are detailed in Article 2, point 1g:

"Insurance and reinsurance undertakings that meet the following criteria in a subsequent manner, identifying:

(i) first, the undertakings exceeding in each of the previous two financial years EUR 500 million of Gross Written Premium (GWP).

(ii) secondly, undertakings that fulfil point (i) included in the 90th percentile of the Gross Written Premiums (GWP) distribution including all undertaking having reported Gross Written Premiums above the average of the Gross Written Premiums of all insurance and reinsurance undertaking established in the Member State calculated separately for the following activities:

- Life other than life Similar-To-Health (SLT) and reinsurance life,
- Non-Life other than non-life Similar-To-Health (NSLT) and reinsurance non-life.- Health calculated as the sum of life Similar-To-Health (SLT) and non-life Similar-To-Health (NSLT),
- Reinsurance calculated as the sum of reinsurance life and reinsurance non-life.

(iii) Third, insurance and reinsurance undertakings that fulfil point (ii) and whose total assets is equal or higher to the 10 % of the sum of the total assets valuated according to Article 75 of Directive 2009/138/EC of the insurance and reinsurance undertakings established in the Member State belonging to the activity type identified as referred to in point (ii)."

Q&A – Subcontracting

Where is the end point for considering subcontractors? What if, for example, Microsoft & Azure do not disclose which subcontractors they use for data center/IT security/software development? Is this the point where I get stuck and need to perform a risk analysis?

The sub-contracting chain never ends - you need to consider all subs until you get stuck, that is right. A risk analysis is the best way to accept the respective risk and have something for external auditors to look at.

Is there a difference between subcontracting and sub-outsourcing (i.e., the subcontractor provides important/relevant services to the outsourced function)?

There is a difference between "Outsourcings" and "ICT services" in general because not all ICT services are an outsourcing and not every outsourcing is in the context of ITC services. There are different discussion on the market at the moment, e.g., if non-IT services should be handled according to EBA // ESM / EIOPA Guidelines and national regulations and IT services according to DORA.

The RTS on subcontracting CI functions Article 1 lays down proportionality. A missing aspect in my view is whether the third-party ICT provider is a critical one or not. Critical third-party ICT providers will be subject to the oversight framework. One would expect this will inform the level of risk. What is your view on this?

There are separate requirements for critical ICT TPSP according to DORA itself. But it is also possible that a critical ICT TPSP is also one supporting critical or important functions. You have to check this first and need a methodology for identifying those critical or important functions.

In your opinion, are some financial services (e.g., postal transactions) to be considered as ICT services and therefore included in the subcontracting chain?

Only those ICT services supporting critical or important functions must be included for all their subs. You need a methodology for identifying those critical or important functions.

Contact

Benny Bogaerts

Partner

T +32 477 30 14 49
bbogaerts@kpmg.com

Benoit Watteyne

Director

T +32 476 66 53 66
bwatteyne@kpmg.com

Thomas Meyer

Director

T +32 471 67 51 57
thomasmeyer@kpmg.com

Sonia Rosu

Senior Advisor

T +32 470 62 60 38
srosu@kpmg.com

Peter Vanderheyden

Senior Advisor
T +32 478 60 08 17
pvanderheyden@kpmg.com

Kris Vancolen

Senior Expert Consultant

T +32 467 01 38 39
kvancolen@kpmg.com

kpmg.com/socialmedia

Global page: [Digital Operational Resilience Act - KPMG Global]