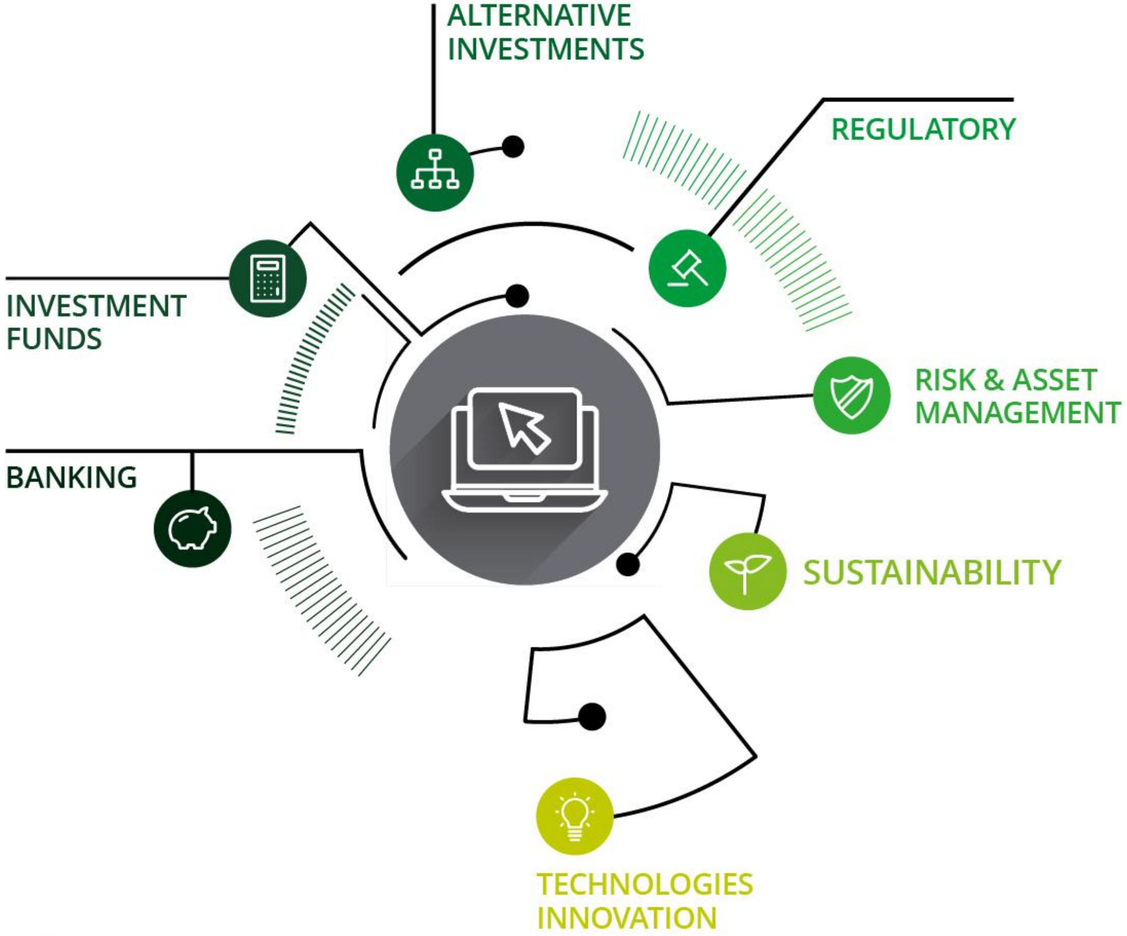
Deloitte.



DORA

Link'n Learn 2023 – 25 October 2023

Getting Started

Here with you today

Laureline Senequier
Partner Digital Risk & Resilience
+352 621 451 843
lsenequier@deloitte.lu

Sébastien Müller-Borle
Senior Manager Digital Risk & Resilience
+352 661 452 339
smullerborle@deloitte.lu

Agenda

1. Context and the 5 DORA Pillars
2. Let’s explore more DORA
3. Closing words

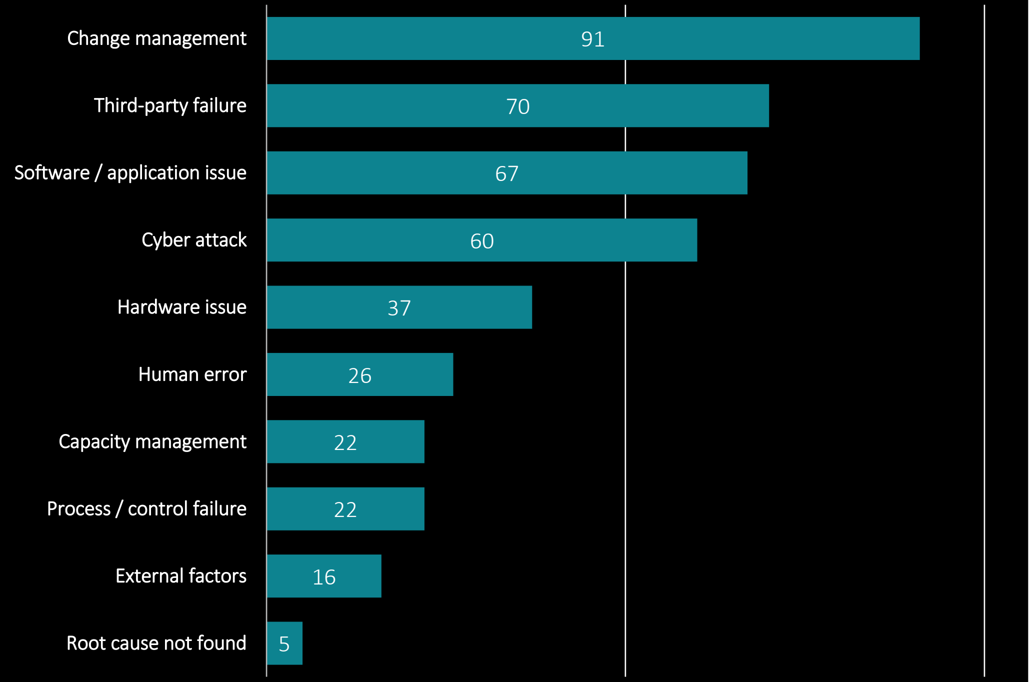
Context and the 5 DORA Pillars

The ICT Earthquakes

Most significant risks in technology in financial services

Known root cause of major technology outages and cyber-attacks

Known root cause of the major technology outages and cyber-attacks reported to the FCA (Financial Conduct Authority) between Oct. 2017 and Sept 2018:



Source: Financial Conduct Authority, 'Cyber and technology resilience: themes from cross-sector survey 2018'

Examples of publicly disclosed major ICT & Security incidents

A major Cloud Provider – Major IT outages due to technical software or hardware issues **(2019)**: A nearly **three-hour global outage** affecting core cloud services that occurred during the migration of a legacy system.

TSB bank - Change management process failure **(2018)** - TSB took all its internet and mobile services offline after a migration to a new platform. **Up to 1.9 million customers locked out of their accounts for six day**. Cost the bank £330m, while 80,000 customers switched their account to a competitor.

Central bank of Bangladesh – Cyber attack **(2016)**: Five successful **fraudulent instructions were issued by hackers** via the SWIFT network to illegally transfer US$ 101 million.

Equifax – Major data breach **(2017)**: Private records of **148 million customers were compromised** in the breach. Many banks had to reissue millions of credit and debit cards that were compromised in the breach.

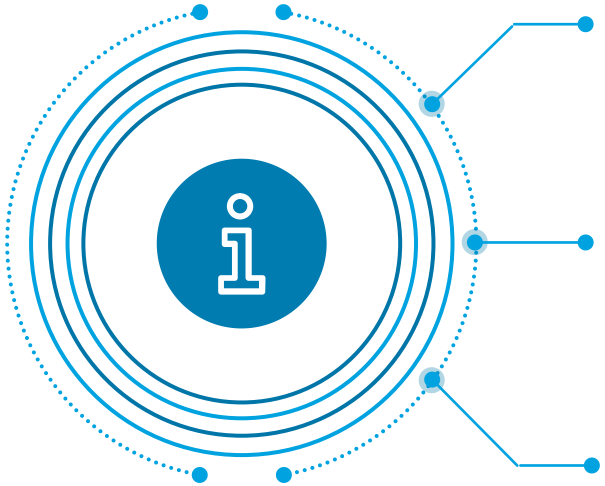
Digital Operational Resilience

The ever-increasing reliance on ICT poses a challenge to the digital operational resilience of the EU financial services.

1 AN EVOLVING LANDSCAPE

- Digital revolution
- System complexity and proliferation of data
- Massive ICT outsourcing and Cloud adoption
- Globally-distributed and interconnected nature of ICT
- New types of cyber-threats

2 FOCUS FROM REGULATORS GOES NOW BEYOND THE ABILITY OF INSTITUTIONS TO ABSORB LOSSES RESULTING FROM ICT INCIDENTS



Financial institution stability
Stability implications of a successful major cyberattack and ability of a financial institution to continue to provide its critical functions.

System-wide risks
Increasing risk of contagion to other institutions and financial services including cyber-threats arising from recourse to third-party service providers

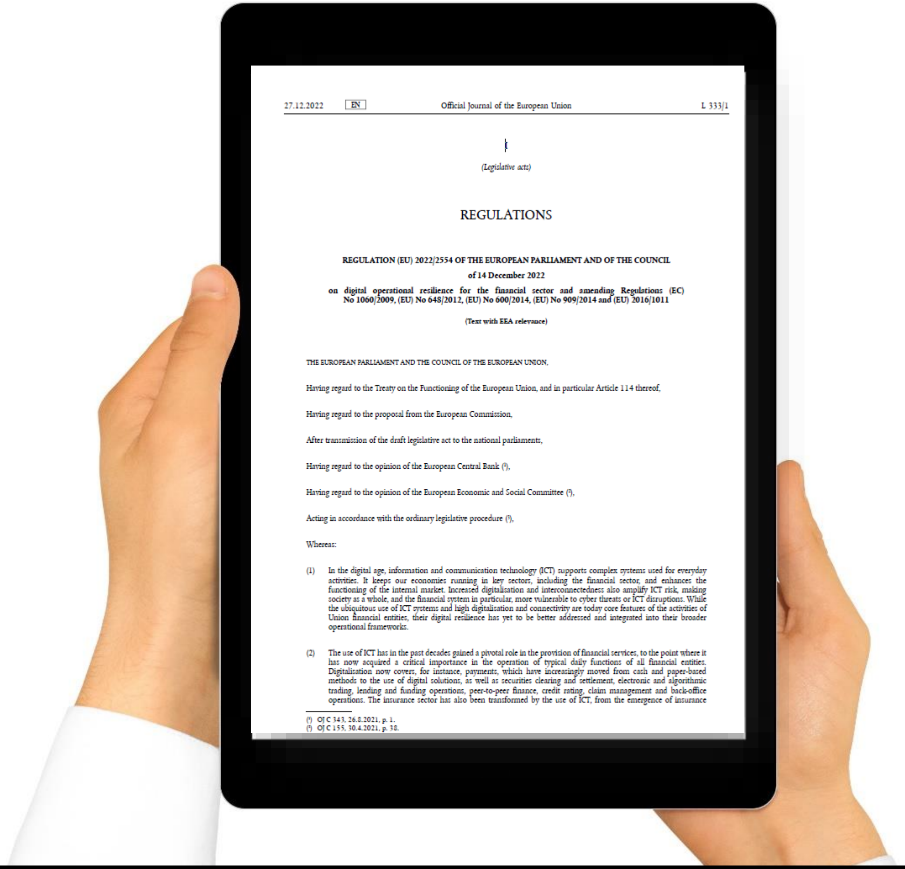
A greater ambition for resilience
Baseline standards are being pushed to challenge entities to become more ambitious in pursuing their cyber-defence and digital operational resilience

✓ **Digital operational resilience** is the ability enabling an institution to (i) **identify and protect** itself from ICT threats and potential failures, **respond and adapt** to, as well as (ii) **recover and learn** from disruptive events in order to minimize their impact on the delivery of critical operations through disruption*

*** Source:** *Basel Committee on Banking Supervision (BCBS) consultative Principles for operational resilience, August 2020*

DORA is the first comprehensive EU Regulation on digital operational resilience

The DORA contains the future architecture of the technical digital requirements needed to support the widespread arrival of technologies, digital assets, and the increased use of data.



27.12.2022 EN Official Journal of the European Union L 333/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank [1],

Having regard to the opinion of the European Economic and Social Committee [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) In the digital age, information and communication technology (ICT) supports complex systems used for everyday activities. It keeps our economies running in key sectors, including the financial sector, and enhances the functioning of the internal market. Increased digitalisation and interconnectedness also amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions. While the ubiquitous use of ICT systems and high digitalisation and connectivity are today core features of the activities of Union financial entities, their digital resilience has yet to be better addressed and integrated into their broader operational frameworks.

(2) The use of ICT has in the past decades gained a pivotal role in the provision of financial services, to the point where it has now acquired a critical importance in the operation of typical daily functions of all financial entities. Digitalisation now covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions, as well as securities clearing and settlement, electronic and algorithmic trading, lending and funding operations, peer-to-peer finance, credit rating, claim management and back-office operations. The insurance sector has also been transformed by the use of ICT, from the emergence of insurance

[1] OJ C 343, 26.8.2021, p. 1.
[2] OJ C 155, 30.4.2021, p. 38.

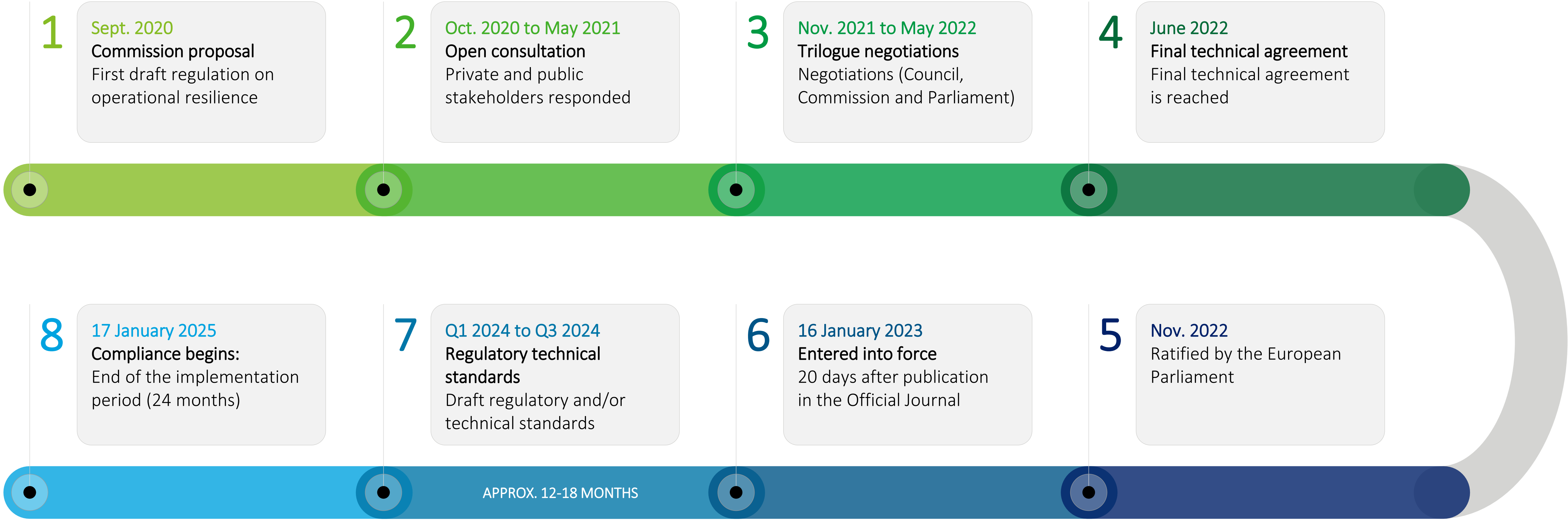
PROPOSAL FOR A DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

- In September 2020, the EU Commission published a legislative proposal for a Digital Operational Resilience Act (DORA). The DORA entered into force on 16 January 2023.
- The objective is to consolidate and upgrade ICT risk requirements throughout the financial sector (incl. Insurance Companies, Asset management, Payment Institutions) to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks.
- DORA builds on the NIS2 directive and addresses possible overlaps via a lex specialist exemption.
- Choice of a Regulation to guarantee a homogenous and coherent application of all components of the ICT risk management by the Union financial sectors.
- Subsequently, the European Supervisory Authorities (ESAs), through the Joint Committee and in consultation with ENISA and the ECB, will develop common draft regulatory technical standards to specify further the requirements applicable to financial entities.

The DORA legislation proposed by the Commission is an important first step in creating a **regulatory framework for financial services' operational resilience in EU law**

Road to implementation

Regulation ratified by the European Parliament and publication in the Official Journal of the European Union will come soon together with the start of the implementation period (24 months).



1 Sept. 2020
Commission proposal
First draft regulation on operational resilience

2 Oct. 2020 to May 2021
Open consultation
Private and public stakeholders responded

3 Nov. 2021 to May 2022
Trilogue negotiations
Negotiations (Council, Commission and Parliament)

4 June 2022
Final technical agreement
Final technical agreement is reached

5 Nov. 2022
Ratified by the European Parliament

6 16 January 2023
Entered into force
20 days after publication in the Official Journal

7 Q1 2024 to Q3 2024
Regulatory technical standards
Draft regulatory and/or technical standards

8 17 January 2025
Compliance begins:
End of the implementation period (24 months)

Scope, objectives and implications of DORA

The DORA, is the first piece of legislation at the EU level addressing the topic of digital operational resilience across the full financial sector.

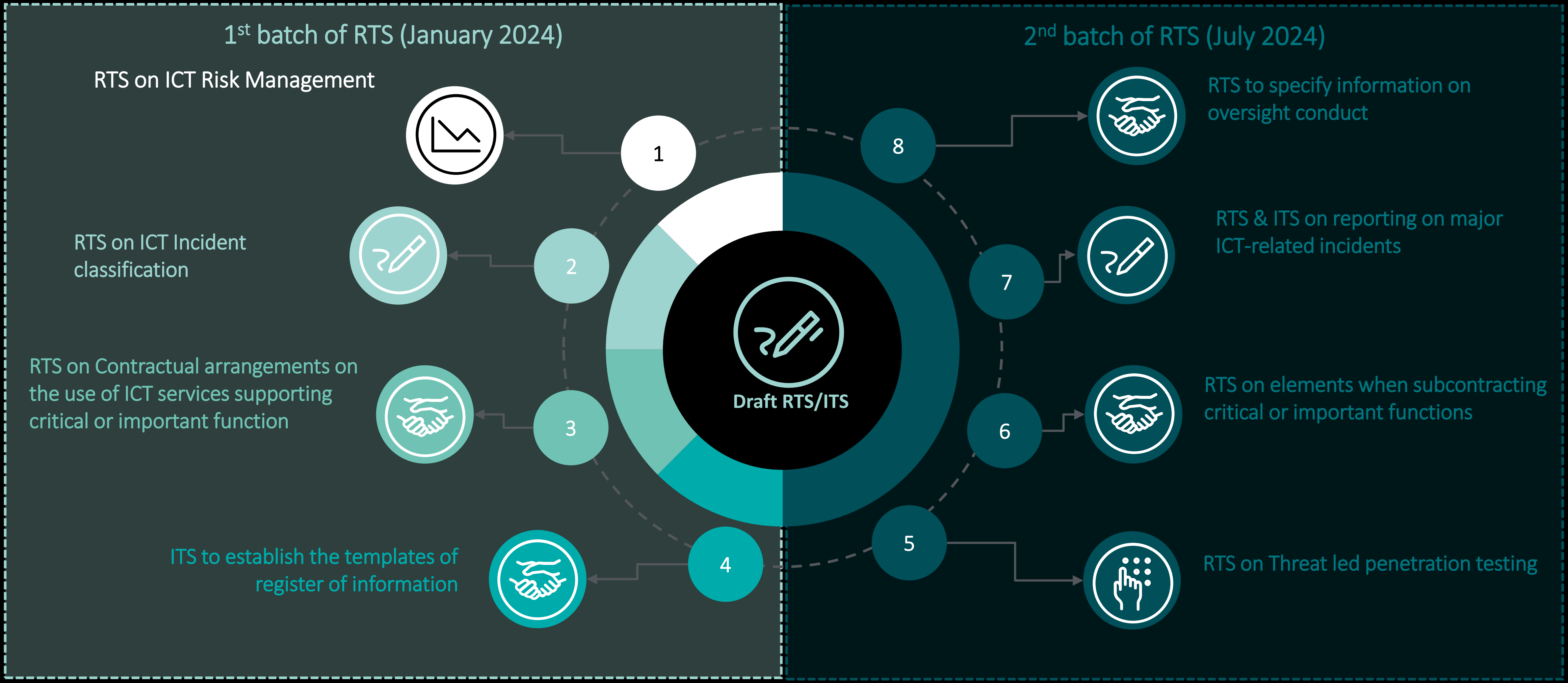
It applies across the full financial sector as well as it **brings within the regulatory perimeter "critical ICT third-party providers"** (CTPPs) who will be supervised by European Supervisory Authorities (ESAs)

FIVE PILLARS	OBJECTIVES	KEY REQUIREMENTS AND IMPLICATIONS	PROPORTIONALITY PRINCIPLE
ICT risk management	Creating an ICT risk management framework around a set of key principles and requirements	• Setting-up an **ICT risk governance** aligned with the 3 Lines of Defense model • Implementing a proportionate **ICT risk management framework** to ensure that ICT risks are identified and managed in a prompt and effective manner • **Board/Top management** extended role and responsibility/accountability	Measures shall be proportionate to the size and overall risk profile, and to the nature, scale and complexity of services, activities and operations
Incident reporting	Harmonising ICT incident classification and reporting	• **Harmonizes multiple incident reporting rules** into a single classification and reporting standard that mandates firms to carefully collect, manage and disseminate incident data. • Mandate for EU supervisors to investigate the potential for a **single EU reporting hub**.	
Digital operational resilience testing	Setting EU-wide standards for digital operational resilience testing	• EU-wide **requirement for resilience testing**, including duty to test all critical functions at least annually and "fully address" any vulnerabilities identified. • Creates a **binding "advanced testing"** requirement for larger firms (Threat-Led Penetration testing) • Require that **Critical Third-Party Parties be involved in some advanced testing**	
ICT third-party risk	Harmonising FS firm's management of third-party risk	• Firms to adopt a **proactive approach stance in ICT Third-Party Risk Management** • **Optional "Holistic Multi-Vendor Strategy"**, but many levers for supervisors to push large firms	
	Creating a direct oversight framework for critical third-party providers	• Sets up a **regime for allowing FS authorities to oversee** and direct Critical Third-Party Providers • **Designated CTPPS to demonstrate their resilience to the ESAs**, which will be able to issue recommendations on improving resilience, and impose fines, etc.	
Information Sharing	Information-sharing arrangements on cyber threat information and intelligence	• Financial entities may **exchange amongst themselves cyber threat information and intelligence**, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools	

Let’s explore more DORA

DRAFT Regulatory Technical Standards

The ESAs launched in Summer 2023 a consultation on the first batch of Regulatory Technical Standards



1st batch of RTS (January 2024)

1. RTS on ICT Risk Management
2. RTS on ICT Incident classification
3. RTS on Contractual arrangements on the use of ICT services supporting critical or important function
4. ITS to establish the templates of register of information

2nd batch of RTS (July 2024)

5. RTS on Threat led penetration testing
6. RTS on elements when subcontracting critical or important functions
7. RTS & ITS on reporting on major ICT-related incidents
8. RTS to specify information on oversight conduct

ICT Risk Management

Incident reporting

Digital operational resilience testing

ICT third-party risk

Draft RTS on ICT risk management tools methods processes & policies

DORA was highly inspired by existing Guidelines (e.g. CSSF Circular 20/750) but RTS provides a higher level of details in the expectations.

RTS Chapter & Article ref.	Chapter I ICT security policies, procedures, protocols and tools									Chapter II Human resources policy and access control (Art. 20 – 22)	Chapter III ICT-related incident detection and response (Art. 23 – 24)	Chapter IV ICT Business Continuity (Art.25– 27)	Chapter V Report on the ICT risk management framework review (Art. 28)
	Provision and governance (Art. 1 & 2)	ICT Risk Management (Art. 3)	ICT Asset Management (Art. 4 & 5)	Encryption and cryptography (Art. 6 & 7)	ICT Operations security (Art. 8-12)	Network security (Art. 13 & 14)	ICT Project and change management (Art.15-17)	Physical and environmental security (Art. 18)	ICT and Information security awareness and training (Art. 19)				
Nb of policies & proc. required	📄	📄 🔄	📄 🔄	📄 X2	📄 🔄 x5	📄 x2 🔄 x2	📄 x2 🔄 x2	📄		📄 x3	📄	📄	
Maping with policies and procedures complying with EBA GL	Ref. to EBA Guideline on ICT and security risk management (EBA/GL/2019/04 & CSSF Circular 20/750)												
	3.2. Governance and strategy	3.3. ICT and security risk management framework	3.5. ICT operations management	3.4.4. ICT operations security	3.4.4. ICT operations security & 3.5. ICT operations management	3.4.4. ICT operations security	3.6. ICT project and change management	3.4.3. Physical security	3.4.7. Information security training and awareness	3.4.2. Logical security	3.4.5. Security monitoring & 3.5.1 ICT incident and problem management	3.7. Business continuity management	NEW

Increase in the requirement's detail level from EBA GL to DORA's RTS

📄 Policies 🔄 Procedures

Draft RTS on ICT risk management tools methods processes & policies

DORA was highly inspired by existing Guidelines (e.g. CSSF Circular 20/750) but RTS provides a higher level of details in the expectations.

Chapter I ICT security policies, procedures, protocols and tools									Chapter II Human resources policy and access control	Chapter III ICT-related incident detection and response	Chapter IV ICT Business Continuity	Chapter V Report on the ICT risk management framework review
Provision and governance	ICT Risk Management	ICT Asset Management	Encryption and cryptography	ICT Operations security	Network security	ICT Project and change management	Physical and environmental security	ICT and Information security awareness and training				

CSSF Circular 20/750

3.4.4. ICT operations security

Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery. These procedures should include the following measures:
[...]
f) encryption of data at rest and in transit (in accordance with the data classification).

From 1 sentence…

RTS on ICT Risk Management

Encryption and cryptography (Art. 6 & 7)

Encryption and cryptography policy must include:

- Rules for encryption of data at rest/ in transit/ in use
- Rules for encryption of internal network connections and traffic with external parties
- Criteria to select cryptographic techniques, use practices considering leading practices
- Provisions to monitor developments in cryptoanalysis

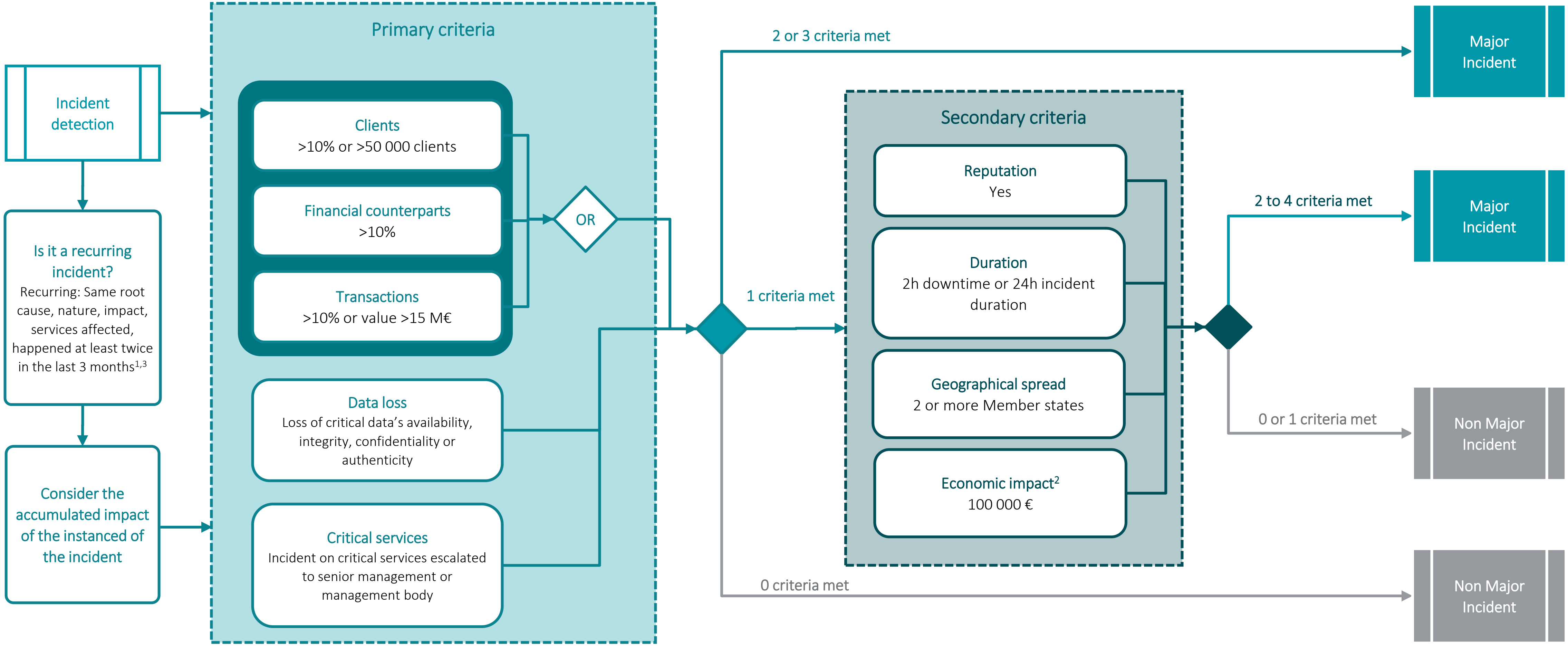
Cryptographic key management policy must include:

- the correct use, protection and lifecycle of cryptographic keys
- Controls to protect cryptographic keys
- Methods to recover cryptographic keys
- Create and keep up to date a register for all certificates and certificate storing devices

… to 1,5 pages

Draft RTS on classification of ICT incidents

Decision tree for classifying an incident or recurring incident[1] as major (Art. 8 to 16)



[1] Incidents or Recurring incidents with criteria in aggregate within the last 3 months.
[2] Direct or indirect gross cost & loss incurred as result of incident.
[3] Up to 12 months for central securities depositories, central counterparties, trading venues, trade repositories, data reporting service providers, credit rating agencies, administrators of critical benchmarks and securitization repositories.

Draft RTS on contractual arrangements on the use of ICT services supporting critical or important function

Draft RTS on contractual arrangements on the use of ICT services supporting critical or important function

ICT Services

- Complexity & risk considerations (Art.1): location of 3rd party, nature of shared data, location of data processing & storage, impact of service disruptions
- Group application (Art.2): if consolidation of financial statements, DORA Article 28 (2) to be implemented for all subsidiaries

A function is **critical or important** if it impacts:

- Compliance, financial performance or continuity of services and activities
- Internal control

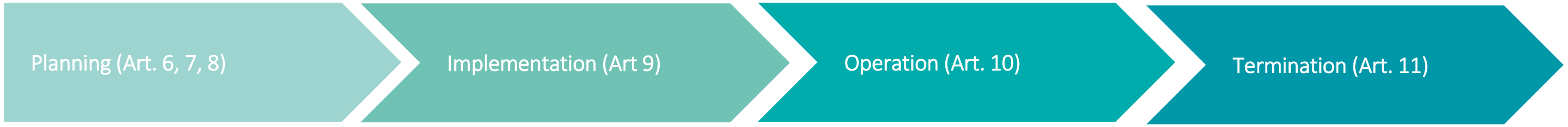
ICT TPP (Article 4): differentiation between

- ICT TPPs authorized & supervised by CA **VS** those that are not
- ICT TPPs intra-group **VS** outside group
- ICT TPPs EU located **VS** outside EU (location of services & location of data)

Governance framework (Art. 3 & Art. 5)

Management body of a financial entity shall adopt & regularly review a written policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. The policy shall include:

- Definition of criticality assessment methodology for ICT services supporting critical or important functions
- Assignment of roles & responsibilities, but also ensure appropriate skills, experience & knowledge
- Oversight over contracted services but also assessment of the provider capacities to avoid legal or regulatory breach
- Definition of role of senior member to monitor contractual arrangements, including reporting to management body
- Consistency of contractual agreements with: ICT risk framework, IS policy, BCM policy and incident reporting requirements
- Requirement for such services to be subject to independent review and part of internal audit plan
- Contracts keep ultimate responsibility with management body, provision cooperation and access of competent authority (CA) & internal audit
- Life cycle of ICT services: decision making / planning / involvement of BU / implementation & monitoring / exit & termination



Planning (Art. 6, 7, 8)

This phase requires:

- Criticality assessment of the ICT Services
- Risk Assessment
- Supervisory condition for contract ICT services
- Due Diligence
- Conflict of interest
- Approval

Implementation (Art 9)

This phase requires:

- Contractual agreement
- Competent authority notification (if required)
- Sub-contracting
- Security measures
- Audit rights
- Termination rights
- Exit Strategy

Operation (Art. 10)

This phase requires:

- Oversight of contracted ICT services
- Exercise Audit rights
- Maintain continuity of ICT services

Termination (Art. 11)

This phase requires:

- Activation of termination clause
- Activation of exit plan
- Service transition

Draft ITS to establish the templates of register of information

Structure and methodology of the register of information: mandatory templates on entity level and (sub)consolidated level

Article 28(9) of the DORA mandates the European Supervisory Authorities (ESAs) to develop draft implementing technical standards to establish the standard templates for the purposes of the register of information, including information that is common to all contractual arrangements on the use of ICT services.

Scope

The ITS on register of information applies to all ICT third party service providers and not only to ICT/Cloud outsourcing (defined in CSSF 22/806).

Register of information at entity level

Contractual arrangements that cover functions of which the financial entity makes use of and is composed of 10 templates. The templates includes information about the financial entity, contractual arrangements (general and specific information), third party service providers, functions identification (including RTO and RPO), etc.

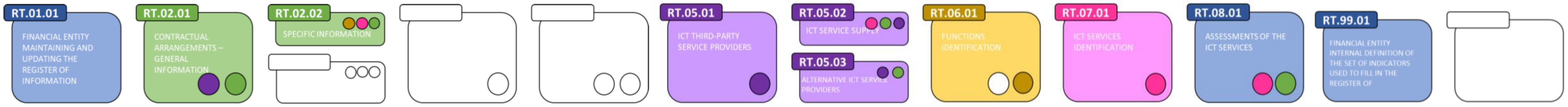
Register of information at sub-consolidated and consolidated level

This contains 14 templates, where 10 out of these 14 templates are the same templates used by financial entities at entity level. The other templates are used to link the registers of information of the various entities in scope of the group and to ensure no double counting (i.e. entities signing the contractual arrangements, entities covered in the scope of the consolidation, etc.)

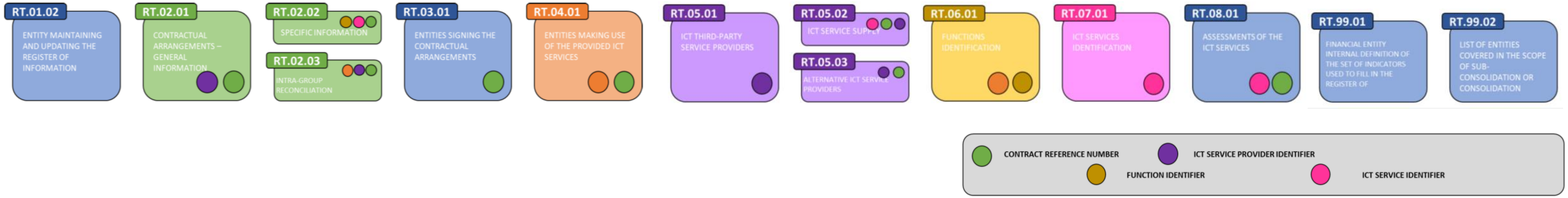
Draft ITS to establish the templates of register of information

Structure and methodology of the register of information: mandatory templates on entity level and (sub)consolidated level

Entity-level


RT.01.01
FINANCIAL ENTITY MAINTAINING AND UPDATING THE REGISTER OF INFORMATION
RT.02.01
CONTRACTUAL ARRANGEMENTS – GENERAL INFORMATION
RT.02.02
SPECIFIC INFORMATION
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

(Sub)consolidated level


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 RECONCILIATION
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
ICT SERVICE PROVIDER IDENTIFIER
FUNCTION IDENTIFIER
ICT SERVICE IDENTIFIER

DORA vs. NIS2 – Lex specialis

European Commission published Guidelines on the equivalence of Cybersecurity requirements in DORA (sector-specific union legal act) with requirements in NIS2 and confirmed Lex Specialis of DORA over NIS2 for Banks & Financial Market Instruments.

DORA Chapter and Article	Entities in scope				NIS2 Chapter and Article
DORA	Investment funds, Insurance, Payment institutions, etc…[1]	Bank & Financial Market Instruments	ICT service providers	Transport, Energy, Health, etc…[2]	NIS2
Chapter I	N/A	N/A	N/A	N/A	**Chapter I to III**
Chapter II – ICT Risk Management **Art 5.** Governance and organisation	●	●	○	○	**Chapter IV - Cyber Security Risk Management Measures and reporting Art 20.** Governance
Chapter II – ICT Risk Management **Art 6 – 16.** ICT Risk Management framework	●	●	○	○	**Chapter IV - Cybersecurity risk management measures** **Art 21.** Cybersecurity risk management measures
Chapter III – ICT Related incident management, classification and reporting Art 17-23	●	●	○	○	**Chapter IV - Cybersecurity risk management measures** **Art 23.** Reporting obligations
Chapter IV – Digital Operational resilience testing **Art 24-27**	●	●	○	○	**Chapter IV - Cybersecurity risk management measures** **Art 24.** Use of European cybersecurity certifications scheme
Chapter V – Managing of ICT Third-party risk **Art 28-30.** Key principles for a sound management	●	●	○	○	**Chapter V - Jurisdiction and Registration** **Art 26-28.**
Chapter V – Critical Third-Party Provider Oversight **Art 31-44.** Oversight Framework	●	▨	▨	○	**Chapter IV – Cybersecurity risk management measures** **Art 22 –** Union level coordinated security risk assessment of critical supply chains
Chapter VI – Information sharing arrangement **Art 45.** Information sharing arrangement on cyber threat	●	●	○	○	**Chapter VI - Information sharing** **Art 29-30**
Chapter VII – Competent authorities **Art 46 - 56**	●	●	○	○	**Chapter VII - Supervision and enforcement** **Art 31-37**
Chapter VIII to IX	N/A	N/A	N/A	N/A	**Chapter VIII to IX**

● *DORA only applies* ○ *NIS2 only applies* ▨ *Both DORA and NIS2 may apply*

Source: EUR-Lex - 52023XC0918(01) - EN - EUR-Lex (europa.eu)

1 – Investment funds, Insurance, Payment institutions, crypto…

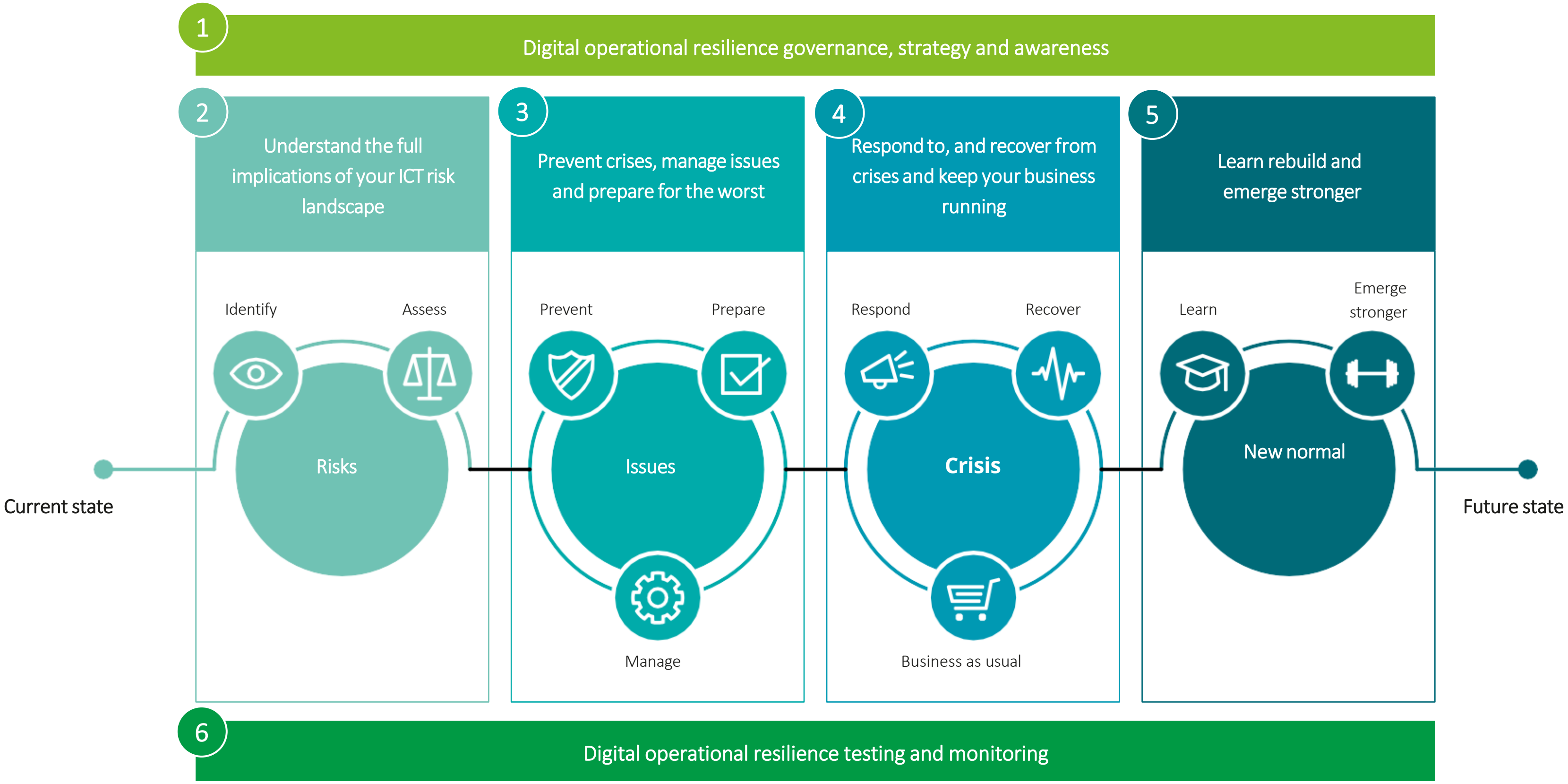
2 – Digital infrastructures, Energy, transport, health, drinking water, wastewater, public administration, space

Closing words

How can Deloitte help?

Deloitte can help along the entire journey towards digital operational resilience and compliance with DORA requirements

By taking a **holistic lifecycle** approach, we can be proactive in meeting financial institution needs and make an impact on their business by helping them to: **identify** and **assess** those ICT risks that can lead to crises; **prevent** controllable risks from escalating; **prepare** for crisis events; and **respond** and **recover** to build the new normal and emerge stronger.


1
Digital operational resilience governance, strategy and awareness
2
Understand the full implications of your ICT risk landscape
3
Prevent crises, manage issues and prepare for the worst
4
Respond to, and recover from crises and keep your business running
5
Learn rebuild and emerge stronger
Identify
Assess
Risks
Prevent
Prepare
Issues
Manage
Respond
Recover
Crisis
Business as usual
Learn
Emerge stronger
New normal
Current state
Future state
6
Digital operational resilience testing and monitoring

Truly effective crisis management goes beyond being reactive and simply protecting existing value.

It also enables **resilience** and powers **future performance**, thereby **enabling an organisation to emerge stronger**.

How can Deloitte help?

A comprehensive set of services to improve ICT Risk management and resilience capabilities, and to ensure compliance with DORA requirements

Deloitte can assist your organization throughout the resilience program to ensure compliance with DORA requirements. In particular, we can (i) **assess your current ICT Risk and resilience posture** (and thus the current level of compliance with DORA requirements), (ii) **define the future desired state**, (iii) **define the roadmap** to reach this future state (and compliance with DORA) and (iv) to **assist in the execution of the roadmap**. Below are some examples of assistance that Deloitte can provide either as part of a comprehensive resilience program or as point solutions:

1 Resilience governance, strategy and awareness

- Define the **digital operational resilience governance and strategy**
- Define and conduct the ICT Risk and Resilience **awareness & education program**

2 Understand the full implications of your risk landscape

- Evaluate the **threat landscape**, identify **critical operations** and map **internal and external assets** that are necessary for their delivery
- Set **risk tolerances for disruptions to critical operations**, and establish service contingencies to maintain business services based on these risk tolerances
- Develop/improve the **ICT Risk management framework** (specifically through a critical operation lens) and perform **regular risk assessments** on legacy systems
- Assistance in **third party risk management**, including updates to the contracts and creation of an oversight framework

3 Prevent crises, manage issues and prepare for the worst

- Define the right set of **preventive measures** (risk-based approach) to prevent incidents from happening

4 Respond to, and recover from crises and keep your business running

- Enhance the **incident management framework** to comply with DORA requirements
- Assistance in **reporting ICT related incidents** to competent authorities
- Improve **continuity and recovery capabilities** (BCP, DRP, etc.) in the light of the threat landscape and risk tolerances for disruptions
- Improve **crisis management capability** and conduct simulation exercises

5 Learn rebuild and emerge stronger

- Lessons learned from past incidents and from testing exercises results, and **improvement of the digital operational resilience framework**

6 Digital operational resilience testing and monitoring

- Design, implement and execute a comprehensive **security testing and assessment program**
- **Perform Threat-Led Penetration Testing**: Threat Intelligence and Red-teaming operations following the TIBER-LU framework
- Design and implement relevant **key risk indicators and dashboard** to measure the effectiveness of ICT risk and resilience capabilities

Questions and answers

Next Link’n Learn webinar

Date: ***08/11/2023***

Topic: **Investment Funds | Asset Servicing Survey 2023**

Deloitte.