KPMG

The journey of DORA

Streamlining third party risk management with ServiceNow TPRM

DORA webinar series – 21/09/2023
KPMG Belgium

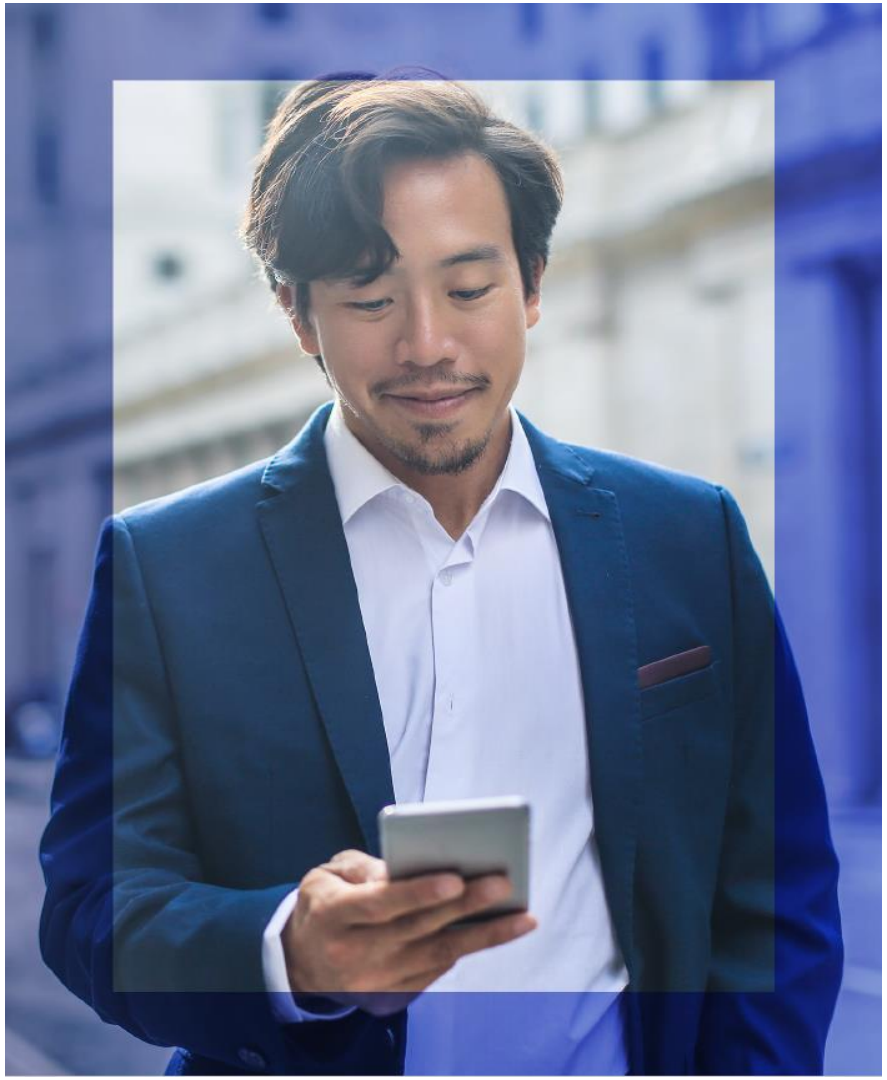
Presenters

Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium

Imène Harrabi

Manager – Procurement, Supply Chain and Third Party Risk Management at KPMG Belgium



Contents

DORA webinar series overview

Today

Streamlining third-party risk mgmt. with ServiceNow TPRM

21-09-2023 | 10:00 - 11:00

Maximizing Resilience with ServiceNow

26-10-2023 | 10:00 - 11:00

Powering your compliance with Security Operations

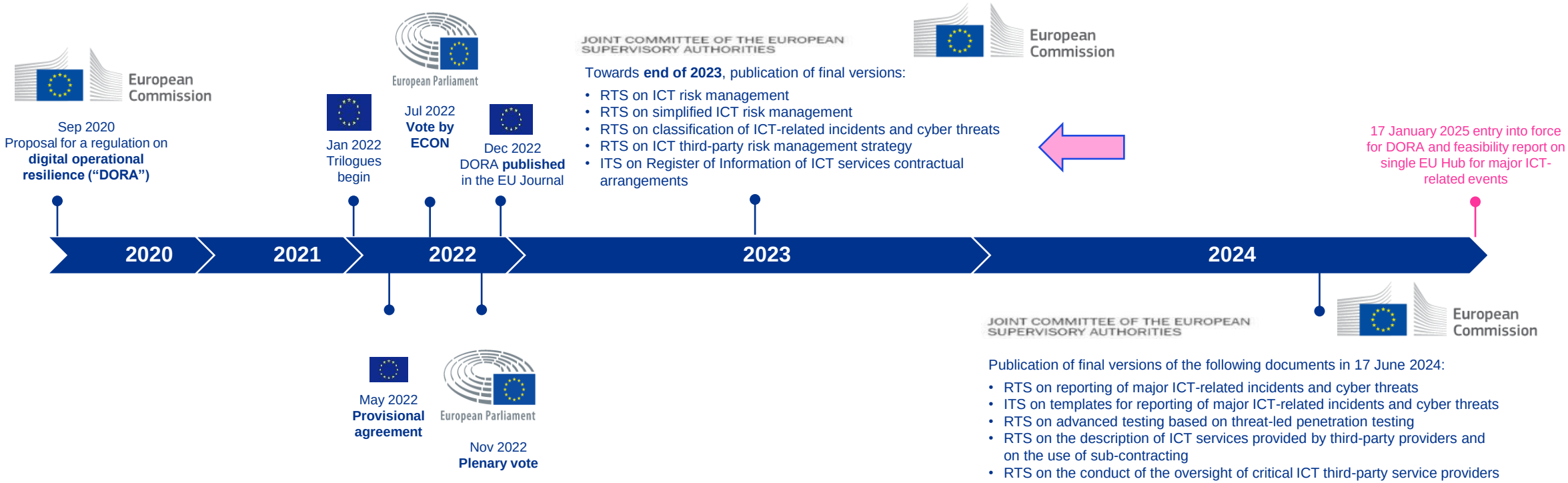
23-11-2023 | 10:00 - 11:30

Upcoming sessions

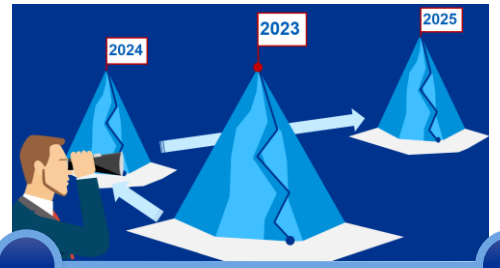
Roadmap to compliance - DORA

EU legislative process and timeline

- The finalization of DORA took place on track and publication in the EU official journal on 27th December 2022.
- This gives organisations a two-year window to assess their compliance and plan the uplift of their internal arrangements by the entry into application of DORA in early 2025.
- In addition, the titles for the consultation papers for the first wave of RTS/ITS/GLs have been agreed.
- The consultation period for the first papers has closed. The publication of the final vesion will be 17 January 2024. Second release will be in Nov/Dec 2023, and finalised by 17 June 2024.



Timeline for Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS)



12 months

DORA regulation put into force January 16, 2023

Finalisation of Wave 1 – 17 January 2024

Mid-June 2023 — **September 2023**

- Development of a consultation document
- Public consultation
- Evaluation of feedback, writing of final report

18 months

- Development of a consultation document
- Public consultation
- Evaluation of feedback, writing of final report

November 2023 — **February 2024**

Finalisation of Wave 2 –17 June 2024

ICT- Risk management framework (Chapter II)	ICT- related incident management, classification and reporting (Chapter III)	Digital Operational Resilience Testing (Chapter IV)	Managing of ICT third- party risk (Chapter V Section I)	Oversight Framework (Chapter V Section II)
RTS for ICT- risk management framework (Art.15)	RTS for classification of ICT-related incidents and cyber threats (Art.18.3)	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)	EBA seeks ESAs' opinion on criticality criteria (Art.31.8) and fees (Art.43.2)
RTS for the simplified ICT risk management framework (Art.16.3)	RTS for the content of the reports od major ICT- related incidents (Art.20.a)		RTS to further specify the detailed content of contractual arrangements (Art.28.10)	Guideline for cooperation between the ESAs and the competent authorities (Art.32.7)
Common guidelines on the estimation of aggregated annual costs and losses (Art.11.11)	ITS for the reporting standards for a financial entity to report a major incident (Art.20.b)		RTS for subcontracting ICT services supporting ICT services supporting critical or important functions (Art.30.5)	RTS for harmonization of the oversight activates(Art.41)
	Feasibility of further centralization of major incident reporting through a single EU- Hub (Art.21)			

Draft submission until 17 January 2024 | Draft submission until 17 July 2024

The six key areas of DORA

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

Focus of today

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

DORA Third party risk management in a nutshell

01 ICT third-party risk as an integral part of the ICT risk management framework

02 Strategy on ICT third-party risk management (TPRM) and lifecycle management

03 Register of Information and understanding your supply chain impact on your CIFs

04 Robust and tested exit and termination clauses

05 Third-parties included as part of resilience and thread-led penetration testing

06 Market supervision of critical third-party service providers

DORA Third party risk management in a nutshell

01 ICT third-party risk as an integral part of the ICT risk management framework

02 Strategy on ICT third-party risk management (TPRM) and lifecycle management

03 Register of Information and understanding your supply chain impact on your CIFs

04 Robust and tested exit and termination clauses

05 Third-parties included as part of resilience and thread-led penetration testing

06 Market supervision of critical third-party service providers

Strategy and TPRM lifecycle management

01 Strategy and Policy

Series of requirements for policy overarching the TPRM activities.

- Scope and Governance
- Definition of ICT services and ICT third-party
- ICT third-party lifecycle
- Risk assessments
- Due diligence
- Conflict of interest
- Contractual clauses
- Ongoing monitoring
- Exit and termination

Additional items like defining supplier mix, use of subcontractors and approach to concentration risk.

NOTE: EBA Guidelines are insufficient in scope and detail – scope of DORA suppliers is much wider

02 Onboarding

- Assessment of concentration risk and possible adoption of multi-vendor strategies
- Due diligence and sources of information:
  - Reputation
  - Locations
  - Conflict of Interest
  - Independent audit reports
  - Certifications
  - Competence of auditors
  - Internal audit
- Contractual requirements such as:
  - exit and termination strategies;
  - right to audit;
  - ethical practices

03 Monitoring

- Assess providers at a defined frequency
- Use measures such as:
  - KPIs
  - Key controls assessment
  - Audits
  - Certifications
  - Security or operational resilience incidents
  - Legal/regulatory compliance
  - Initiate steps if breached or service degradation
  - Regular risk assessments and performance management
  - Resilience testing and thread-led penetration testing

NOTE: Intra-group suppliers are to be treated as third-party

04 Exit/termination

In place for suppliers supporting CIFs.

Termination to be considered for: breaches of law; changes impacting performance; evidenced weaknesses in security; cannot be supervised by authorities

Exit strategies must have some specific criteria:

- failure or deterioration of services, disruption, material risks, or termination of contract
- ensure no impact to service or compliance
- documented and tested
- alternative solutions and transition plan for services and data

Supply chain compliance approach, analysis, and treatment

1. Identify

Map suppliers involved in supporting Critical and Important functions

Review ongoing RFIs and RFPs to assess potential need to include ad-hoc arrangements

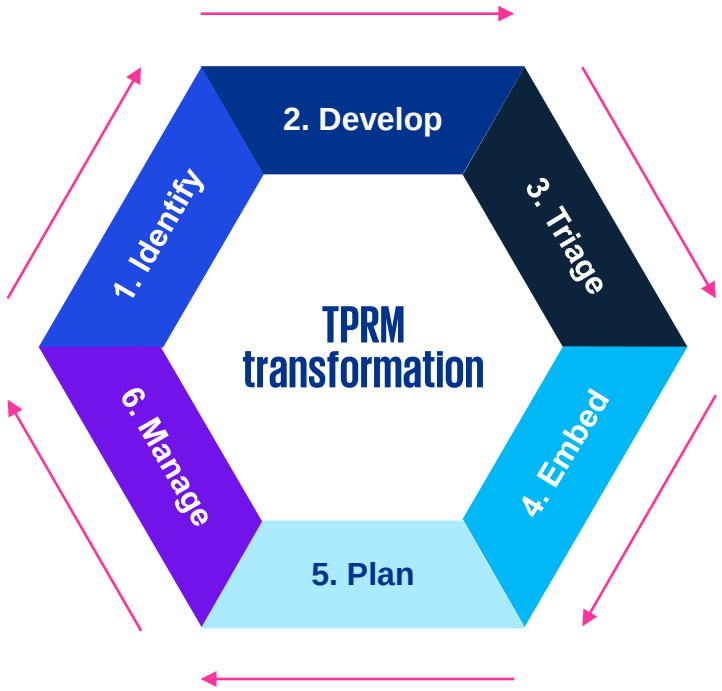
2. Develop approach and TOM

Your approach needs to consider the relevant policy items, but also how you will plan/prioritise against the current supplier base.

Given not all suppliers can be fully addressed in the timeframe, this work should also identify how you will manage the risk of not having all items in place.

3. Initial Assessment and triage

Your in-scope supplier base should be assessed based on your policy, approach, and TOM – the resulting gap analysis will form the basis of the planning, as well as your risk treatment.



4. Process transformation and embedding

The defined model and processes need to be embedded into your standard processes and incorporated into in-flight projects.

5. Supplier planning

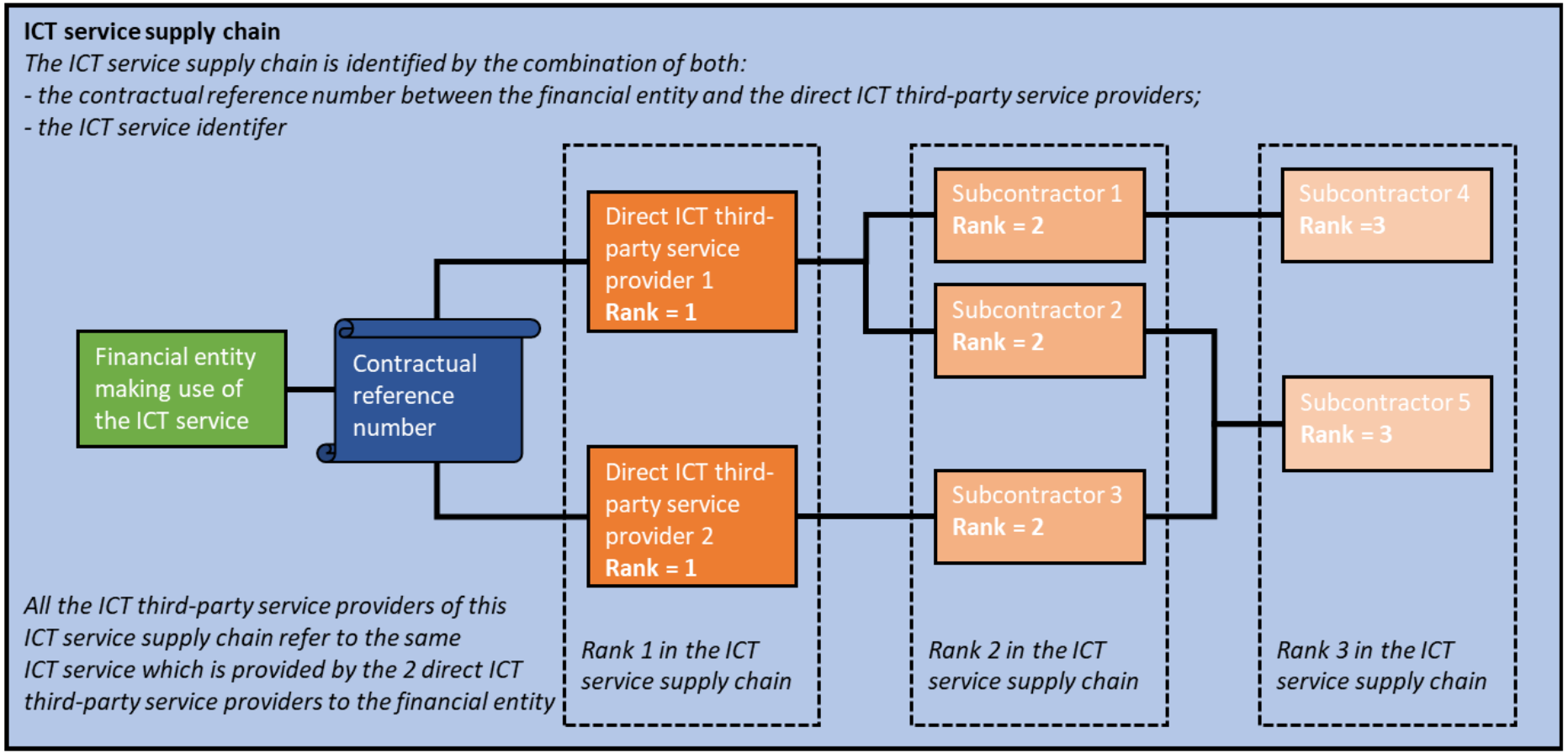
Using contract lifecycle information coupled with the initial assessment output, a prioritised plan to both gather initial supply-chain information for the register of information, as well as contractual uplift, and audit/assessment activity needs to be compiled. This will act as the remediation plan to be followed, tracked, and updated over the coming years.

6. Supplier management

As per the plan, the suppliers will need to be contacted.

Initial priority is to obtain information needed for the register of information, but also communicate the desired approach and enter into negotiation about timing, requirements, exist clause development, remediation, testing, monitoring and reporting.

ICT Service Supply Chain overview



What are the practical implications of these requirements?

Under DORA, financial entities will be required to manage risks in connection with providers of ICT related services. In practise, this means that the following information, relationships and activities need to be managed and performed:

Adopting a policy on the use of third-party ICT services concerning critical or important functions

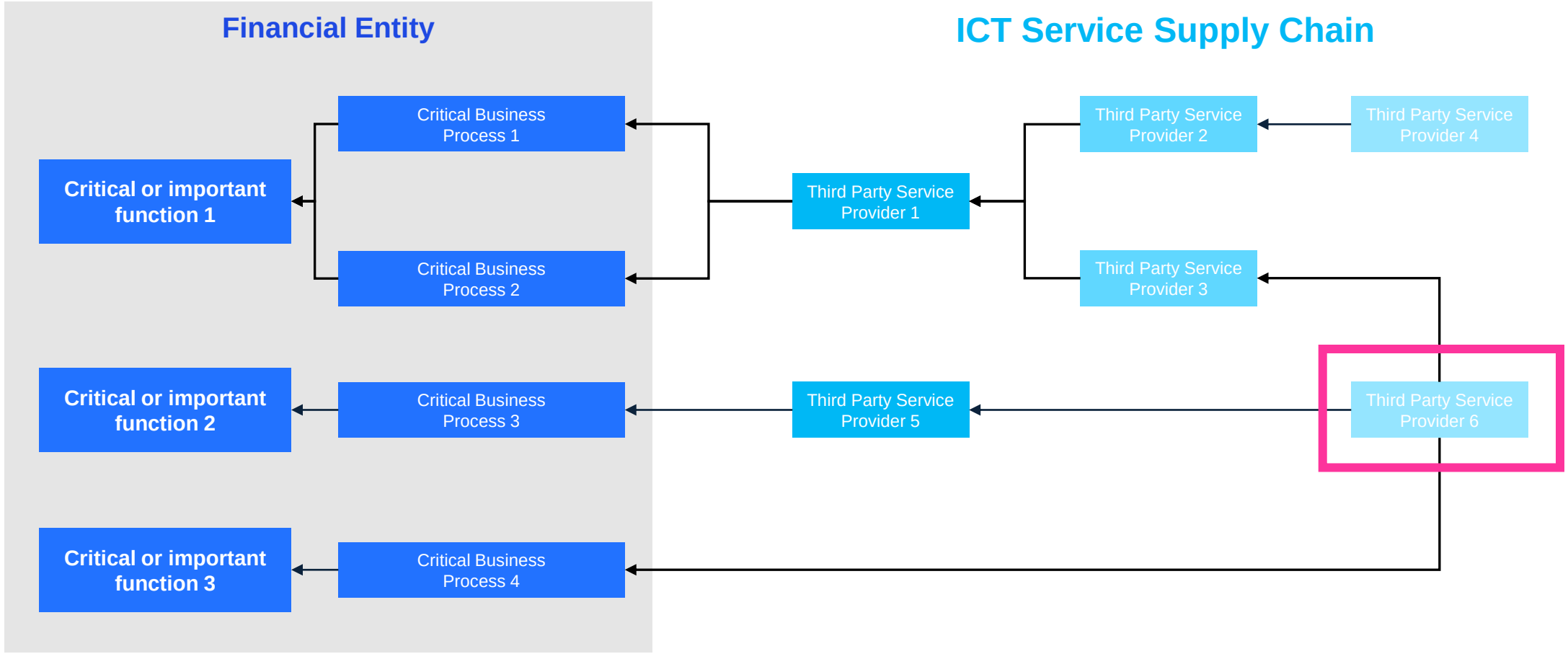
- Scope and Governance requirements (Articles 1–3)
- Definition of ICT services and ICT third-party (Article 4)
- ICT third-party lifecycle requirements (Article 5)
- Risk assessments requirements (Article 6)
- Due diligence requirements (Article 7)
- Conflict of interest requirements (Article 8)
- Contractual clauses requirements (Article 9)
- Ongoing monitoring requirements (Article 10)
- Exit and termination requirements (Article 11)

Establishing a register of all ICT-related contractual arrangements

- RT.01.02 Financial entity maintaining the register of information
- RT.02.01 Contractual Arrangements – General Information
- RT.02.02 Contractual Arrangements – specific information
- *RT.02.03 List of intra-group contractual arrangements and links with contractual arrangements with ICT third-party service provider which are not part of the same group*
- *RT.03.01 Entities signing the Contractual Arrangements for receiving ICT service(s) or on behalf of the entities making use of the ICT service(s)*
- *RT.04.01 Entities making use of the ICT services Objective of this template is to list all entities making use of the ICT services provided by the ICT third-party service*
- RT.05.01 ICT third-party service providers
- RT.05.02 ICT service supply chains
- RT.05.03 Alternative ICT third party service providers
- RT.06.01 Functions identification
- RT.07.01 ICT services identification
- RT.08.01 Assessments of the ICT services
- RT99.01 Definitions from Entities making use of the ICT Services
- *RT99.02 List of financial entities within the scope of sub consolidation and consolidation*

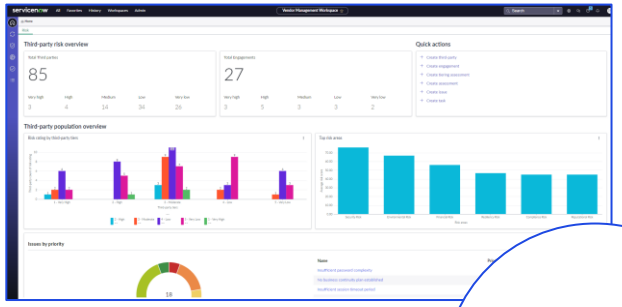
You need to identify and manage the relationship between your third parties and your critical or important functions

Mapping third party service providers to your critical and important functions



Demo – Managing relationships between third parties and business services

Vendor Management Workspace



Downstream suppliers

Subsidiaries

Assessments

Tiering

Due diligence

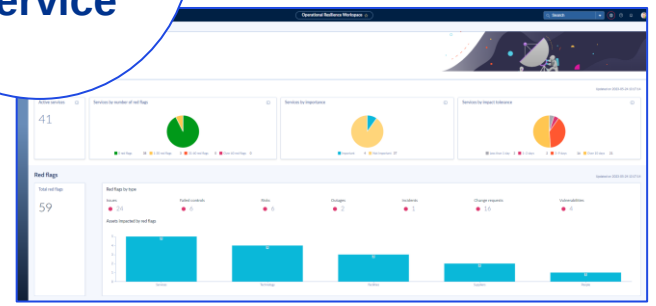
Third Parties

Critical or Important Service

Business Impact Assessment

Business Continuity Plan

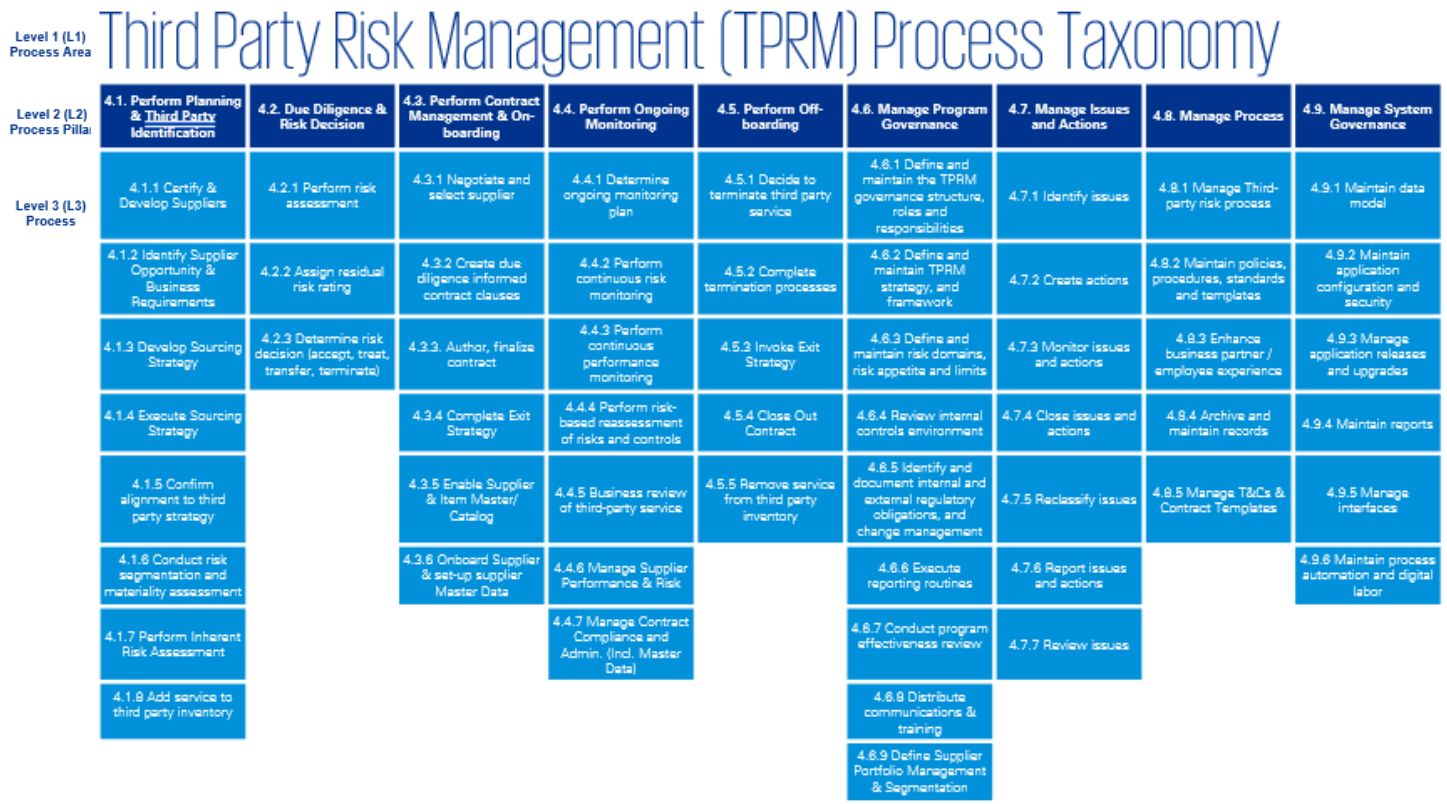
Impact & tolerance Assessment



Operational Resilience Workspace

DORA needs to be grounded in your TPRM framework

Third party risk management, when done properly, will be the result of solid operational risk management.The more mature your TPRM framework is, the easier it will be to stay resilient.



Key points to consider

01. ICT Third party risk management is a key **focus area** for the regulator.

But it is not just something you will do because the regulator asks you so. You want to manage your Third party risks because you want to be able to **achieve your companies' objectives** in a competitive and (sometimes) hostile world.

02.

03. TPRM, when done properly, will be the **result of robust relationship with your vendors**.

04. For good TPRM management, the **tooling** is a key facilitator. When you think about tooling, you might realize that some areas of your framework are less mature.

05. For all typical areas that constitute the ideal **TPRM framework**, we can help you conduct a **maturity assessment**, chart out a roadmap and help you **implement the roadmap**. Our Target Operating models cover all components of the framework

Next webinars

Next up

Maximizing Resilience with ServiceNow

26-10-2023 | 10:00 - 11:00

Powering your compliance with Security Operations

23-11-2023 | 10:00 - 11:30

Establishing a solid governance framework with ServiceNow

25-05-2023 | 10:00 - 11:00

Navigating the IT Risk landscape with ServiceNow

22-06-2023 | 10:00 - 11:00

Streamlining third-party risk mgmt. with ServiceNow TPRM

21-09-2023 | 10:00 - 11:00

Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium

thomasmeyer@kpmg.com

Imène Harrabi

Manager – Procurement, Supply Chain and Third Party Risk Management at KPMG Belgium

iharrabi@kpmg.com

Hans Meulmeester

Director – GRC Solutions (Governance, risk and compliance) at KPMG Belgium

hmeulmeester@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Document Classification: KPMG Public