The journey of DORA

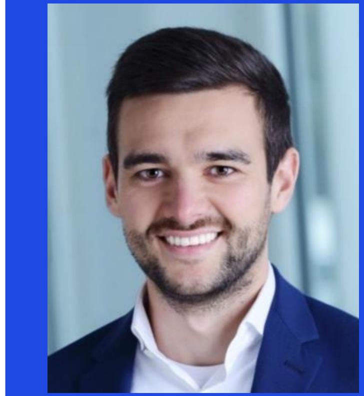
Maximizing Resilience with ServiceNow

DORA webinar series – 26/10/2023
KPMG Belgium

Presenters

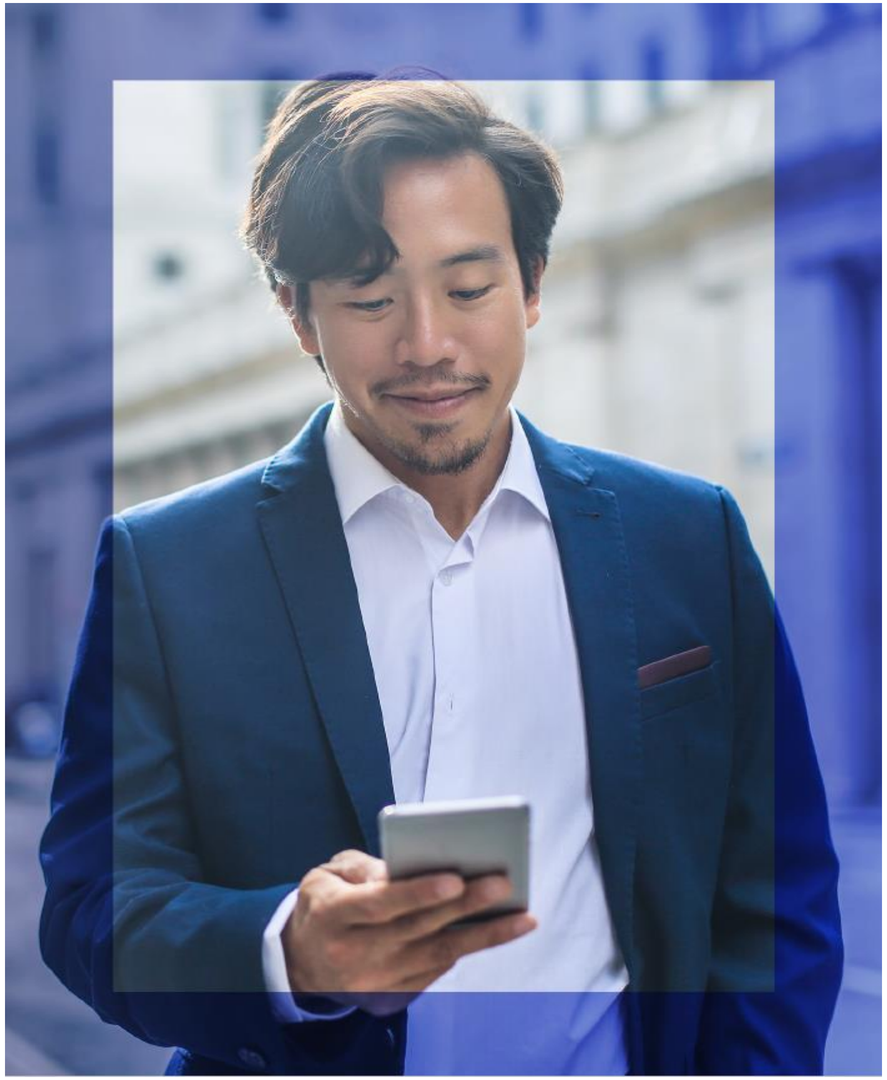
Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium



Dimitri Van Hoolst-Matthyssen

Senior Manager – Solution Lead Powered Risk with ServiceNow at KPMG Belgium



Contents

01 The journey of DORA

02 DORA Governance area deep dive

03 Operational Resilience in ServiceNow

04 ServiceNow demo

05 Recap and next topics

DORA webinar series overview

Today

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

01

The journey of DORA

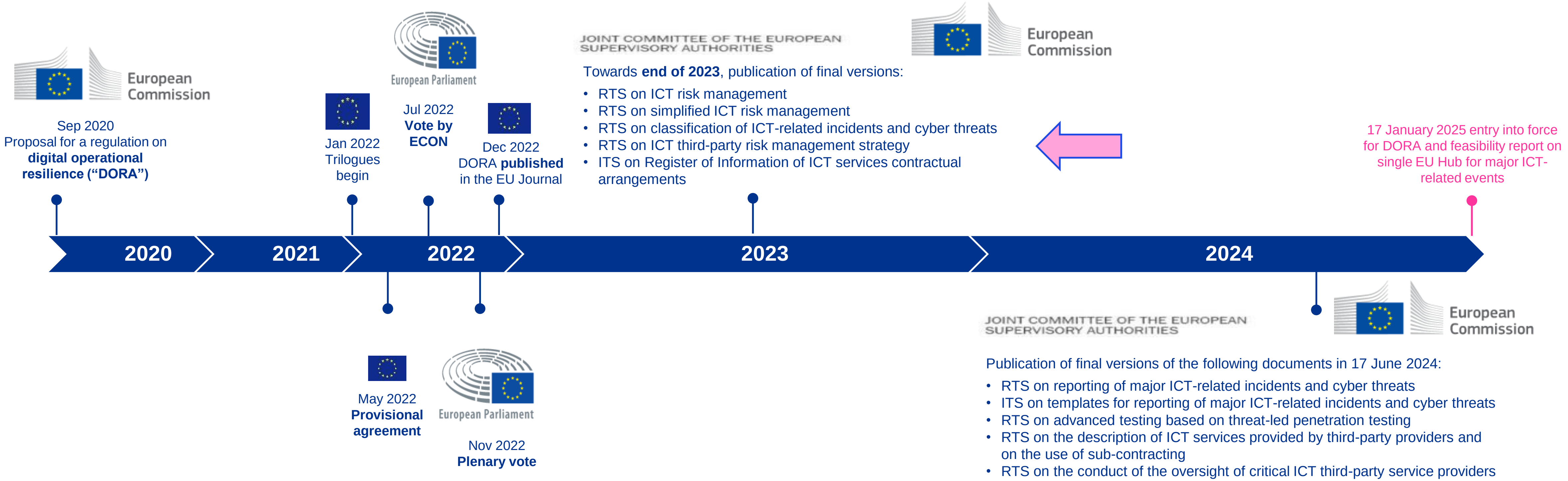
DORA is not a “one-off” compliance exercise, but will push you to get and remain resilient.

Achieve not just short-term regulatory compliance, but also strategic resilience, by creating a scalable and sustainable operating model for the longer term, developing true accountability and embedding a resilience culture.

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.



Sep 2020
Proposal for a regulation on **digital operational resilience (“DORA”)**

Jan 2022
Trilogues begin

May 2022
Provisional agreement

Jul 2022
Vote by ECON

Nov 2022
Plenary vote

Dec 2022
DORA **published** in the EU Journal

Towards **end of 2023**, publication of final versions:

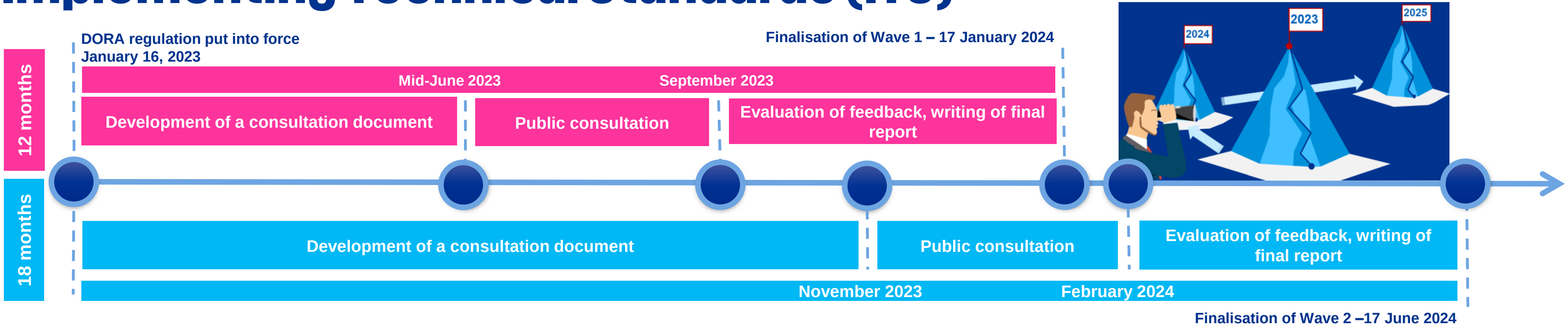
- RTS on ICT risk management
- RTS on simplified ICT risk management
- RTS on classification of ICT-related incidents and cyber threats
- RTS on ICT third-party risk management strategy
- ITS on Register of Information of ICT services contractual arrangements

Publication of final versions of the following documents in 17 June 2024:

- RTS on reporting of major ICT-related incidents and cyber threats
- ITS on templates for reporting of major ICT-related incidents and cyber threats
- RTS on advanced testing based on threat-led penetration testing
- RTS on the description of ICT services provided by third-party providers and on the use of sub-contracting
- RTS on the conduct of the oversight of critical ICT third-party service providers
- Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents

17 January 2025 entry into force for DORA and feasibility report on single EU Hub for major ICT-related events

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)

- 🔴 RTS for ICT- risk management framework (Art.15)
- 🔴 RTS for the simplified ICT risk management framework (Art.16.3)
- 🔵 Common guidelines on the estimation of aggregated annual costs and losses (Art.11.11)

ICT- related incident management, classification and reporting (Chapter III)

- 🔴 RTS for classification of ICT- related incidents and cyber threats (Art.18.3)
- 🔵 RTS for the content of the reports od 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)

Digital Operational Resilience Testing (Chapter IV)

- 🔵 RTS for advanced testing of ICT tools, systems and processes based on TLPT (Art.26.11)

Managing of ICT third- party risk (Chapter V Section I)

- 🔴 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 ICT services supporting critical or important functions (Art.30.5)

Oversight Framework (Chapter V Section II)

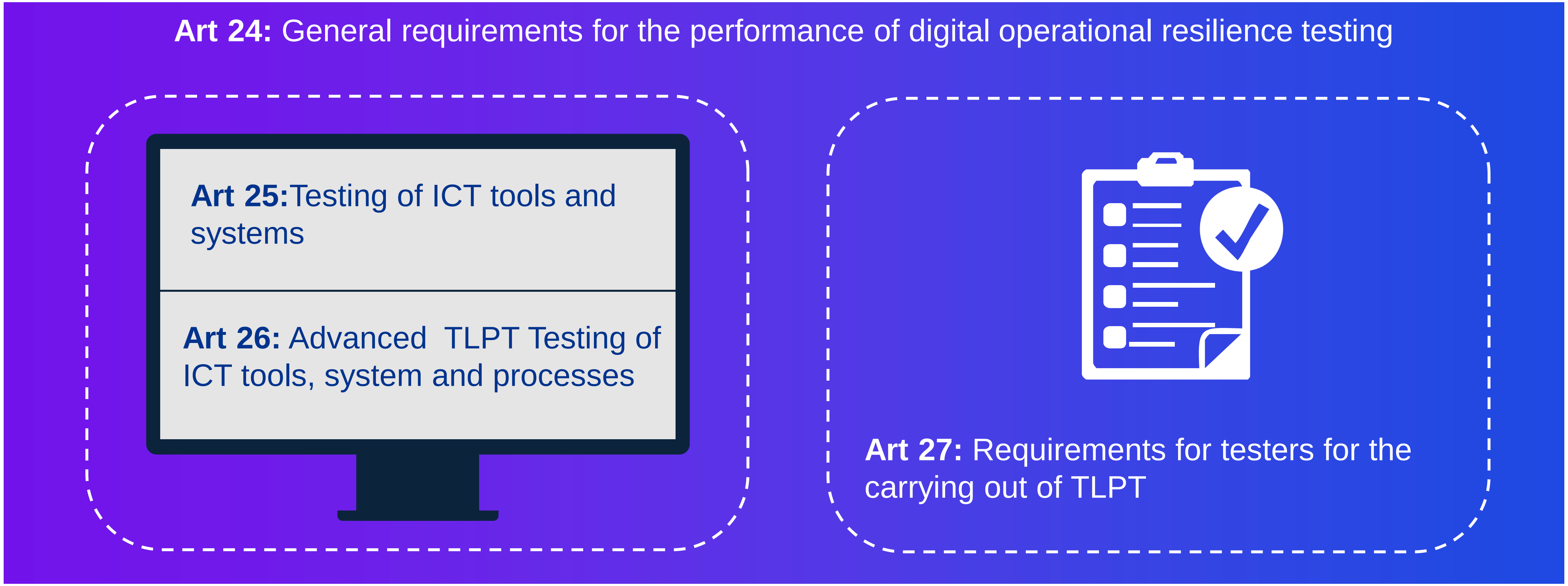
- 🔵 EBA seeks ESAs' opinion on criticality criteria (Art.31.8) and fees (Art.43.2)
- 🔵 Guideline for cooperation between the ESAs and the competent authorities (Art.32.7)
- 🔵 RTS for harmonization of the oversight activates(Art.41)

🔴 Draft submission until 17 January 2024 🔵 Draft submission until 17 July 2024

02

DORA and Operational Resilience

Chapter 4 provides requirements, tools and processes on how digital operational resilience testing should be executed



Art 24: General requirements for the performance of digital operational resilience testing

Art 25: Testing of ICT tools and systems

Art 26: Advanced TLPT Testing of ICT tools, system and processes

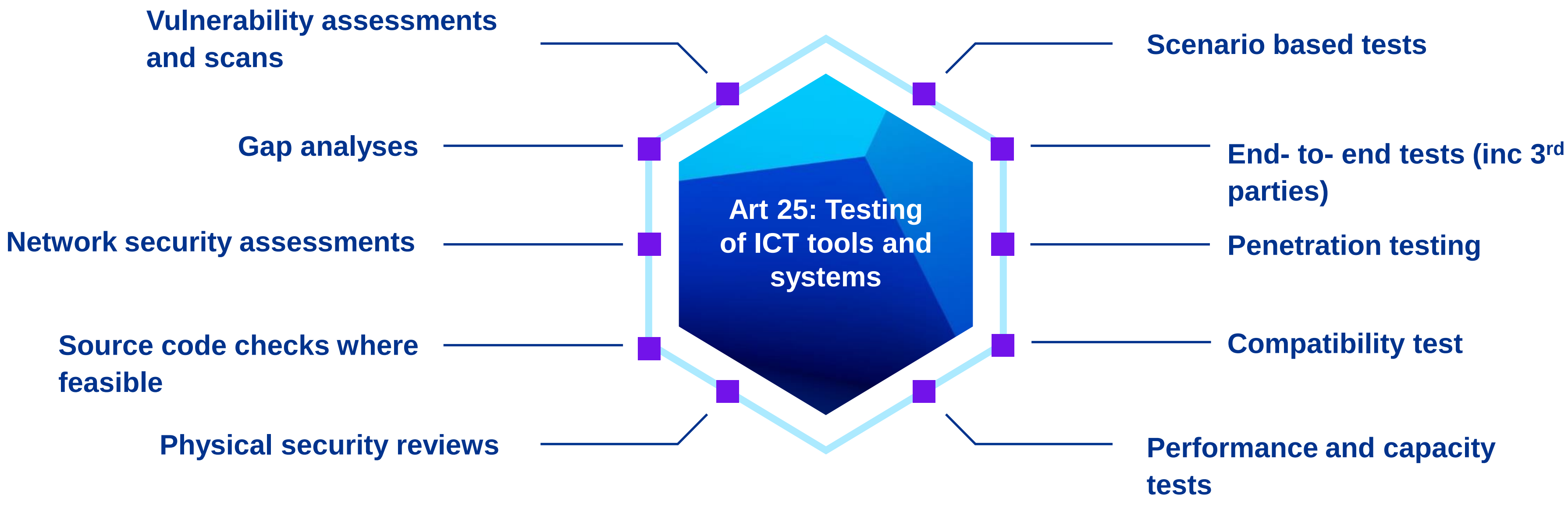
Art 27: Requirements for testers for the carrying out of TLPT

Testing requirements – an integral part of the ICT risk management framework

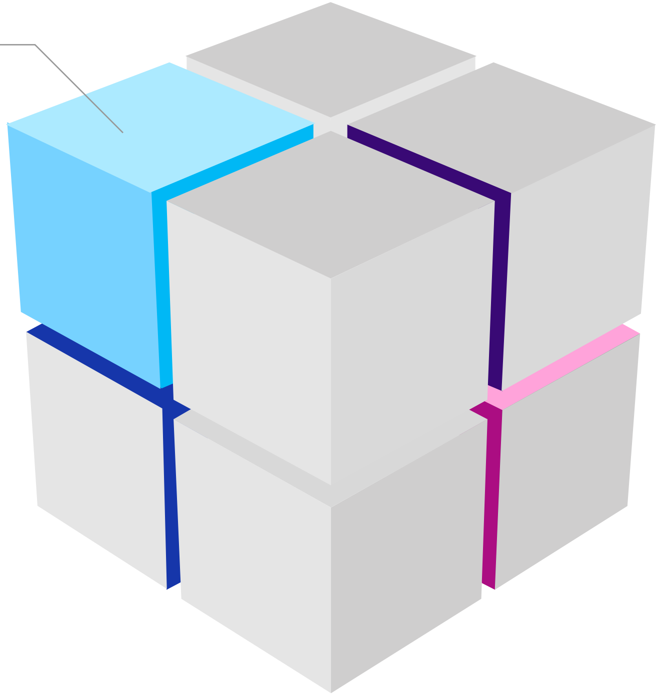
Articles 24 & 25

Article 24 - General requirements

- **Proportionality**: the program must be appropriate to the size, profile and risk profile of the company (risk-based approach)
- **Testing** of all critical ICT systems & applications at least once per year
- **Independence:** financial companies ensure that all tests are performed by independent internal or external parties


Art 25: Testing of ICT tools and systems
Vulnerability assessments and scans
Gap analyses
Network security assessments
Source code checks where feasible
Physical security reviews
Scenario based tests
End- to- end tests (inc 3rd parties)
Penetration testing
Compatibility test
Performance and capacity tests

Operational Resilience and BCM evolved



Business Continuity Management and Disaster Recovery

Traditional coverage, with data centre and recovery testing, along with standalone BIAs and site-map

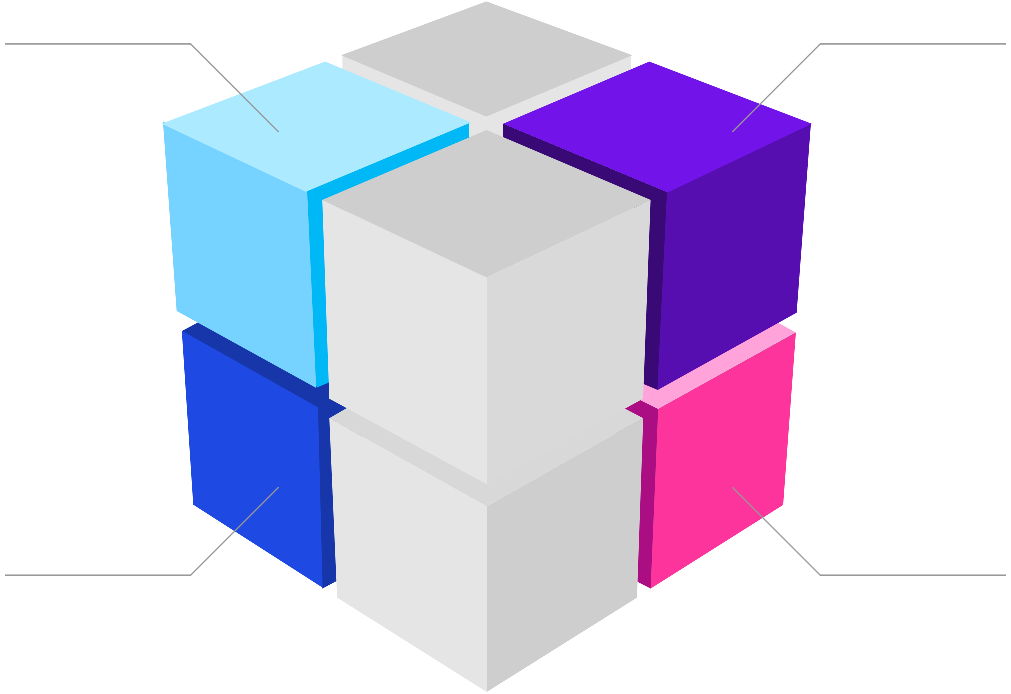
Operational Resilience and BCM evolved

Operational Resilience – BCM, DR +

Now key integration and oversight mechanism. Movement from a BCM/DR approach, to a holistic and integrated function working with cross-discipline teams to provide assurance over the organisational resilience.

Threat-led penetration testing and scenario testing

Threat-led penetration testing is mandated for specific organisations identified by the competent authorities. However, use of scenario-led testing to help structure the most valuable elements of testing is needed



Security testing

Security testing and assessments act as input into resilience planning. This includes physical tests, source code reviews, vulnerability scanning, penetrating testing and more.

End-to-testing and beyond

A key feature of the DORA requirements is around end-to-end testing of the critical and important functions. This not only involves ICT elements within the organisation that directly support the operation, but the underlying technologies and third party providers involved in the service. This integrated element, along with parts such as performance and capacity testing.

Critical and important functions require a higher testing frequency than noncritical or important functions

	Testing of ICT Business Continuity Plans	Other tests within the digital operational resilience testing program	Threat Led Penetration Tests
Critical or important functions	Yearly (Art. 11(6))	Yearly (Art. 24(6))	Every 3 years (Art. 26(1))
Noncritical functions		TBD	

TLPT only needs to be performed if identified by competent authority

Chapter 4 covers how advanced testing (TLPT) is done and the requirements for testers

Articles 26 & 27

Applies only to certain companies that have been identified by the competent authorities

Advanced testing of ICT tools, systems and processes based on TLPT (Article 26)

Frequency of the extended tests:

- At least every three years

After completion of testing:

- Reports and plans with remedial action is submitted

Competent Authorities:

- Identify financial entities, that are required to conduct TLTP

Testing:

- relevant ICT processes, systems and technologies to support critical functions and services
- On live production systems
- Scope approved by authority

Requirements for testers (Art 27):

- high suitability and reputability
- covered by relevant professional indemnity insurances
- provide an independent assurance, or an audit report

When using **internal testers**:

- use has been approved by the relevant competent authority
- threat intelligence provider is external to the financial entity

Essential functions or services delegated to third parties:

- Advanced testing must be performed for third-party services

DORA Operational resilience testing in a nutshell

01

A proportional and risk-based approach

The plan should use a variety of means to ensure coverage and proportional management of risk

02

Integrated into risk management framework

Operational Resilience testing is a key component and a practical way of making the risk management activity concrete – results and follow-up must be included in the overall risk management framework for the organisation.

03

Beyond traditional testing to include cyber and end-to-end testing with third-parties

Include vulnerability assessments, open-source information, code reviews, performance and capacity testing and more.

04

Threat-led penetration testing for relevant entities, and scenario-based testing

TLPT needs specific criteria and accredited testing teams to perform the test. May involve multiple organisations including critical third party providers.

03

ServiceNow & DORA

Key areas of DORA mapped to ServiceNow

Below we can see how the modules of ServiceNow map to the 6 key areas of DORA

IRM

Ops. Res.

ITOM

Governance requirements

- **IRM** (Integrated Risk Management)
- **Operational resilience**
- **ITOM** (IT Operation Management)

SecOps

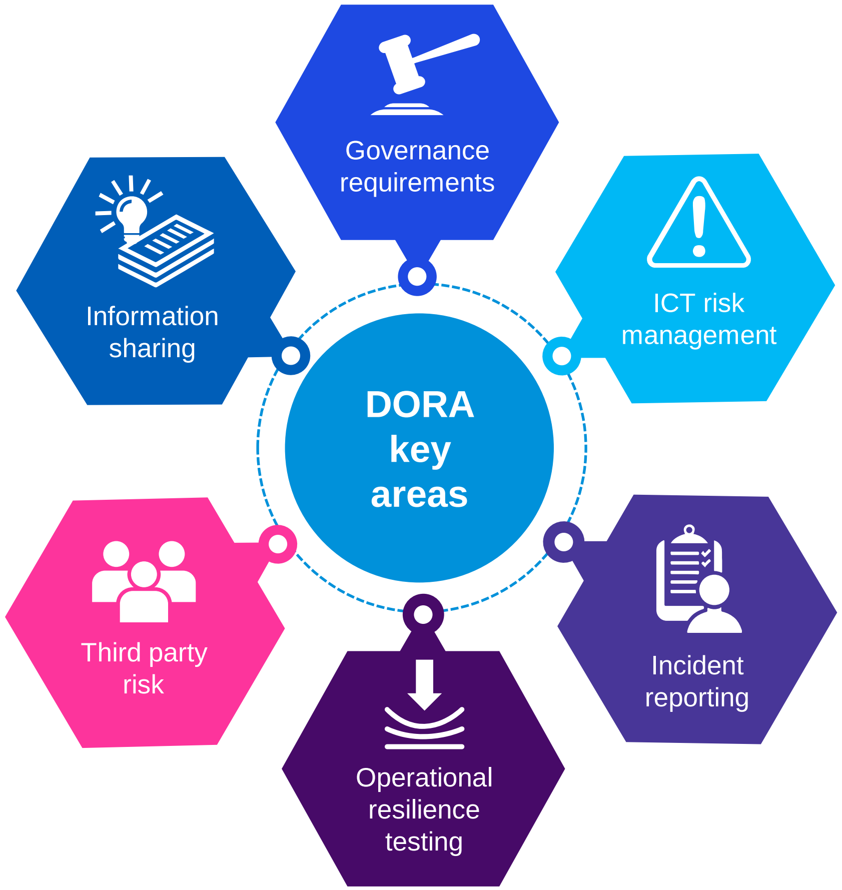
Information sharing

- **SecOps** (Security Operations)

VRM

Third party risk

- **VRM** (Vendor Risk Management)



ICT risk management

- **IRM** (Integrated Risk Management)
- **BCM** (Business Continuity Management)

IRM

BCM

Incident reporting

- **ITSM** (IT Service Management)
- **SecOps** (Security Operations)
- **IRM** (Integrated Risk Management)

ITSM

SecOps

IRM

Focus of today

Operational resilience testing

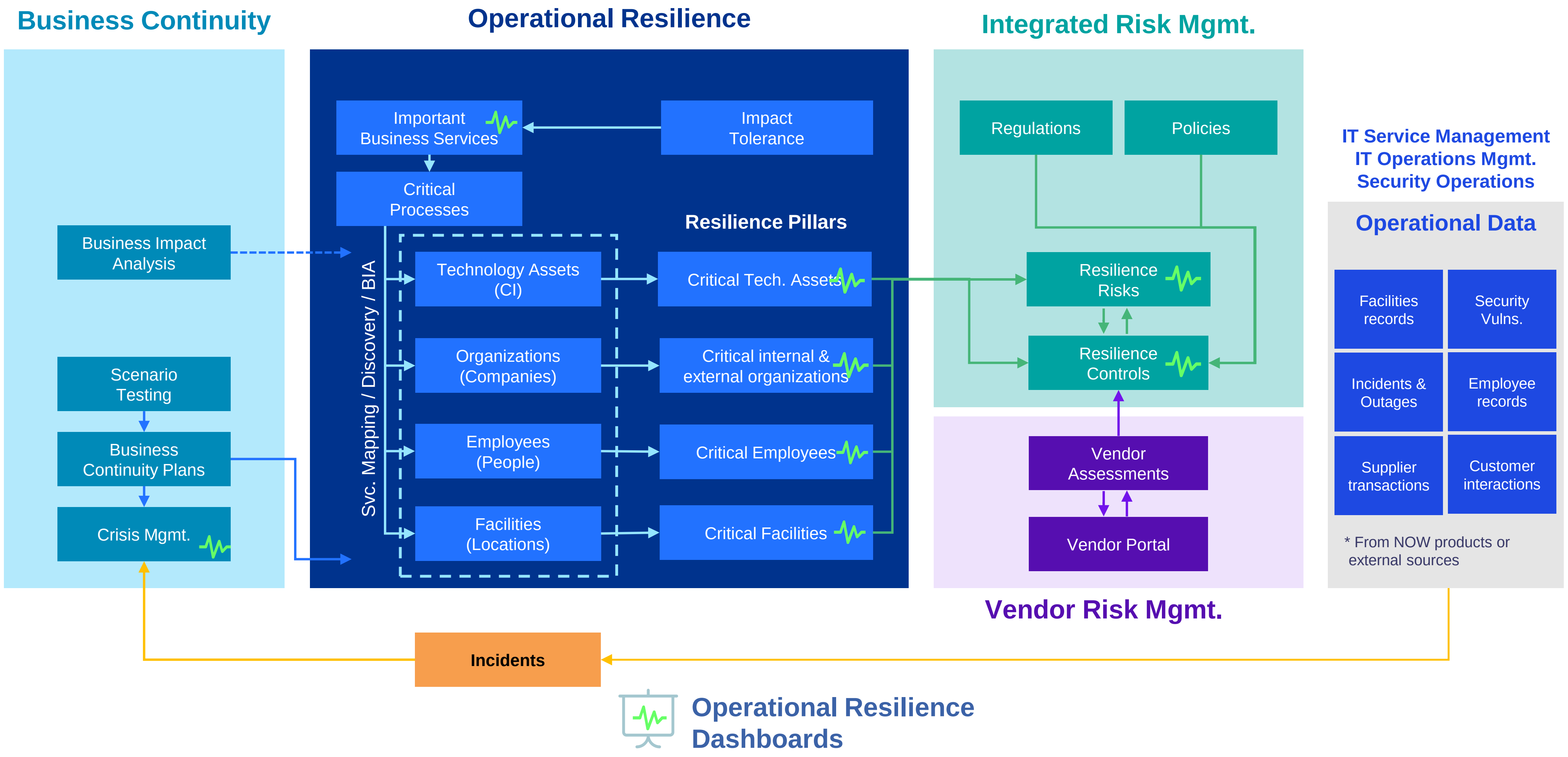
- **Operational resilience**
- **BCM** (Business Continuity Management)

Ops. Res.

BCM

KPMG

The operational resilience workflow in ServiceNow



DORA requires you to manage the connections between services, processes, and assets

Article 7

Identification

As part of the ICT risk management framework referred to in Article 5(1), financial entities shall identify, classify and adequately document all ICT-related business functions, the information assets supporting these functions, and the ICT system configurations and interconnections with internal and external ICT systems. Financial entities shall review as needed, and at least yearly, the adequacy of the classification of the information assets and of any relevant documentation.

Article 22

Testing of ICT tools and systems

.... Financial entities referred to in points (f) and (g) of Article 2(1) shall perform vulnerability assessments before any deployment or redeployment of new or existing services supporting the critical functions, applications and infrastructure components of the financial entity.

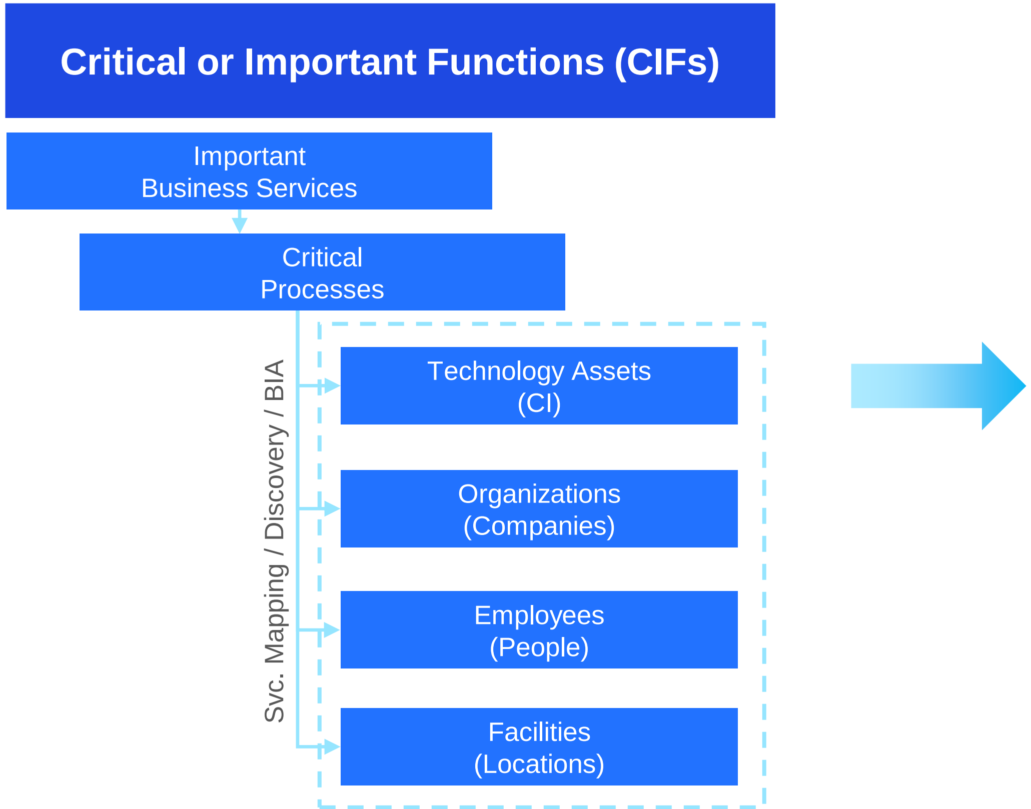
Article 23

Advanced testing of ICT tools, systems and processes based on threat led penetration testing

… For the purpose of the first subparagraph, financial entities shall identify all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or contracted to ICT third-party service providers. …

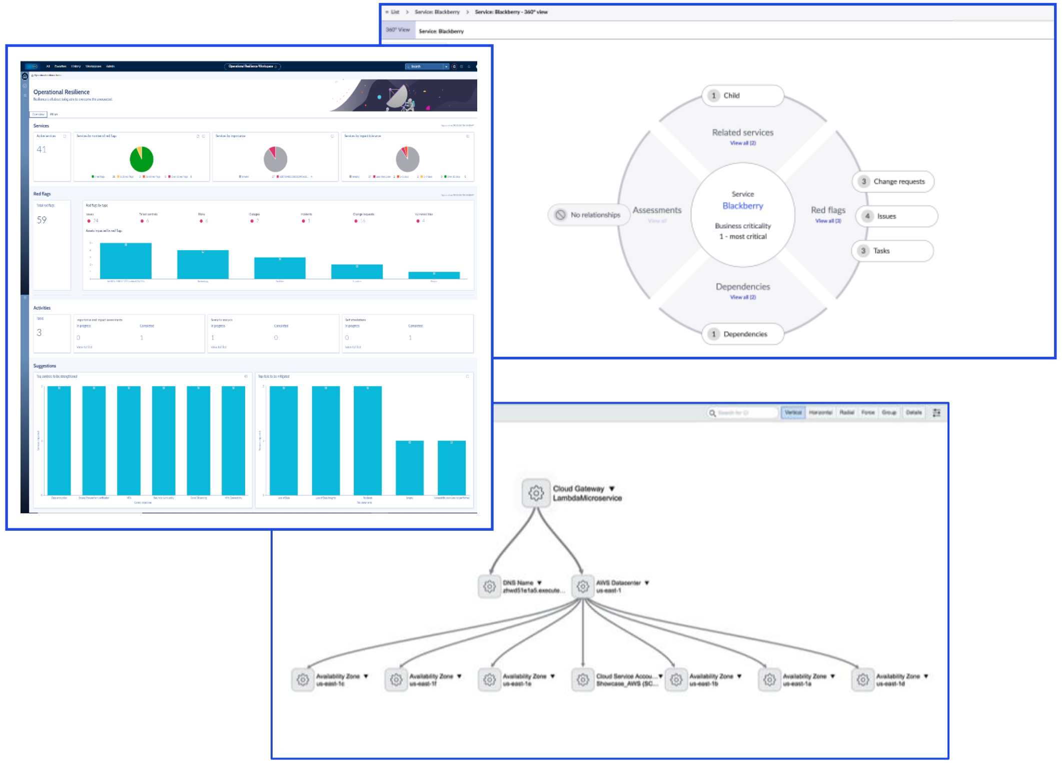
Critical or Important Functions as a base for DORA compliancy

You need to identify the critical or important IT functions and map the related assets, third parties and interdependencies. This becomes significantly more efficient and insightful when using technology.



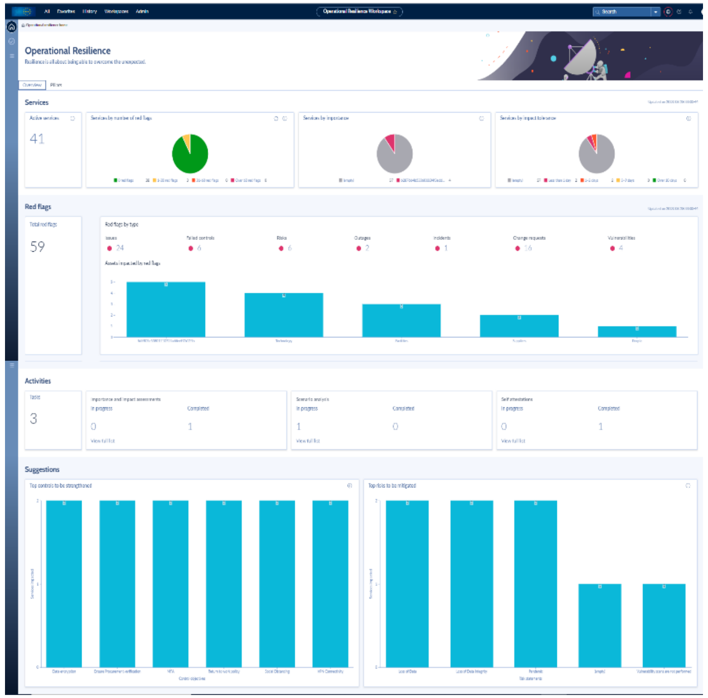
Critical or Important Functions (CIFs)
Important Business Services
Critical Processes
Svc. Mapping / Discovery / BIA
Technology Assets (CI)
Organizations (Companies)
Employees (People)
Facilities (Locations)

Reporting

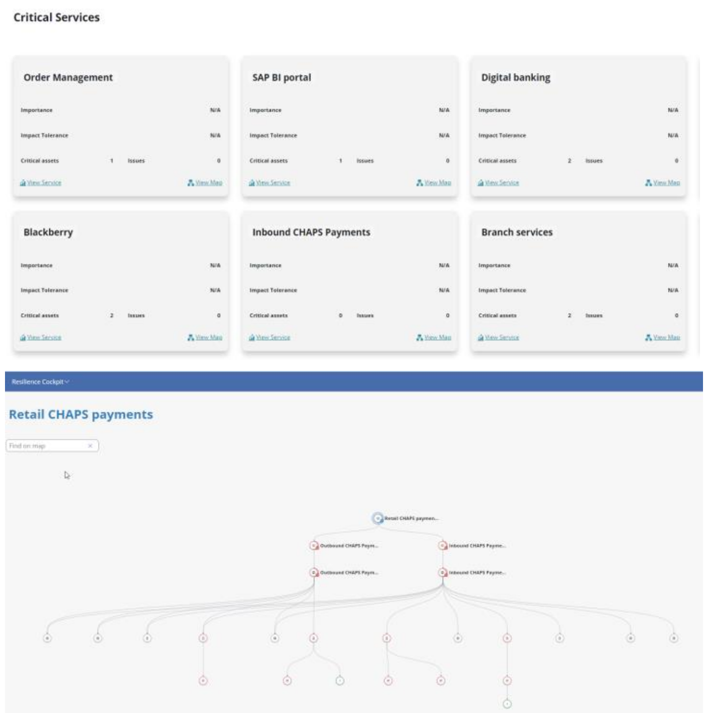


ServiceNow demo – Operational Resilience

Operational Resilience Workspace



KPMG Operational Resilience Cockpit



Critical Services

Order Management

Importance			N/A
Impact Tolerance			N/A
Critical assets	1	Issues	0
View Service			View Map

SAP BI portal

Importance			N/A
Impact Tolerance			N/A
Critical assets	1	Issues	0
View Service			View Map

Digital banking

Importance			N/A
Impact Tolerance			N/A
Critical assets	2	Issues	0
View Service			View Map

Blackberry

Importance			N/A
Impact Tolerance			N/A
Critical assets	2	Issues	0
View Service			View Map

Inbound CHAPS Payments

Importance			N/A
Impact Tolerance			N/A
Critical assets	0	Issues	0
View Service			View Map

Branch services

Importance			N/A
Impact Tolerance			N/A
Critical assets	2	Issues	0
View Service			View Map

Resilience Cockpit

Retail CHAPS payments

- End-to-end data visualization
- Access to historic mapping data

04

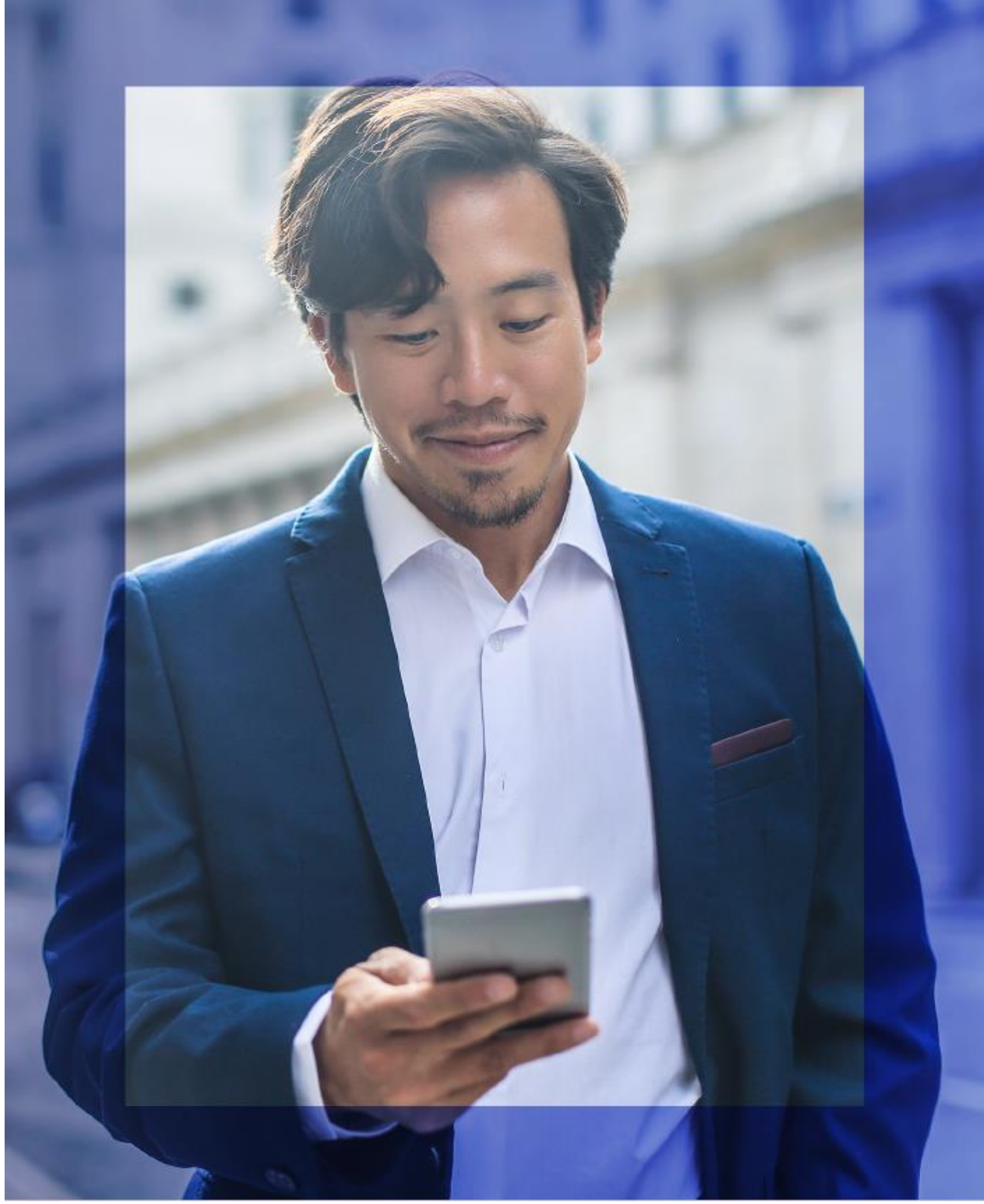
ServiceNow Demo

05

Next steps

Operational Resilience is not a solution, but rather an outcome that you achieve.

- Establishing streamlined business processes is crucial, and the technology platform will effectively facilitate their implementation.
- DORA necessitates the consolidation of data from various areas within the organization, potentially involving different data sources.
- Establishing connections between services, processes, and assets is essential but challenging without appropriate tools.
- Implementing an integrated platform with a unified data model will greatly enhance the efficiency of your DORA reporting.



Next webinar

Next up

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

Maximizing Resilience with ServiceNow

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

Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium

thomasmeyer@kpmg.com

Dimitri Van Hoolst-Matthyssen

Senior Manager – Solution Lead Powered Risk with ServiceNow at KPMG Belgium

dvanhoolst@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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Document Classification: KPMG Public

Next steps to get started

01. **Setup** – establish a DORA programme for 2024 and appoint a programme director and sponsor

02. **Assess** – set strategic goals, perform your readiness and gap assessment

03. **Mobilise** – engage organisational teams and create the supporting structures. Identify your target maturity state and key dependencies

04. **Harmonise** – develop a prioritised remediation programme, which includes process harmonisation. Create detailed requirements and select tools such as ServiceNow, to support transformation in-line with your strategic goals

05. **Institutionalise and embed** – deliver the remediation programme, turn the transformation into sustainable practice, operationalising your technology platform