



# The journey of DORA

**Establishing a solid  
governance framework  
with ServiceNow**

DORA webinar series – 25/05/2023  
KPMG Belgium

# Presenters



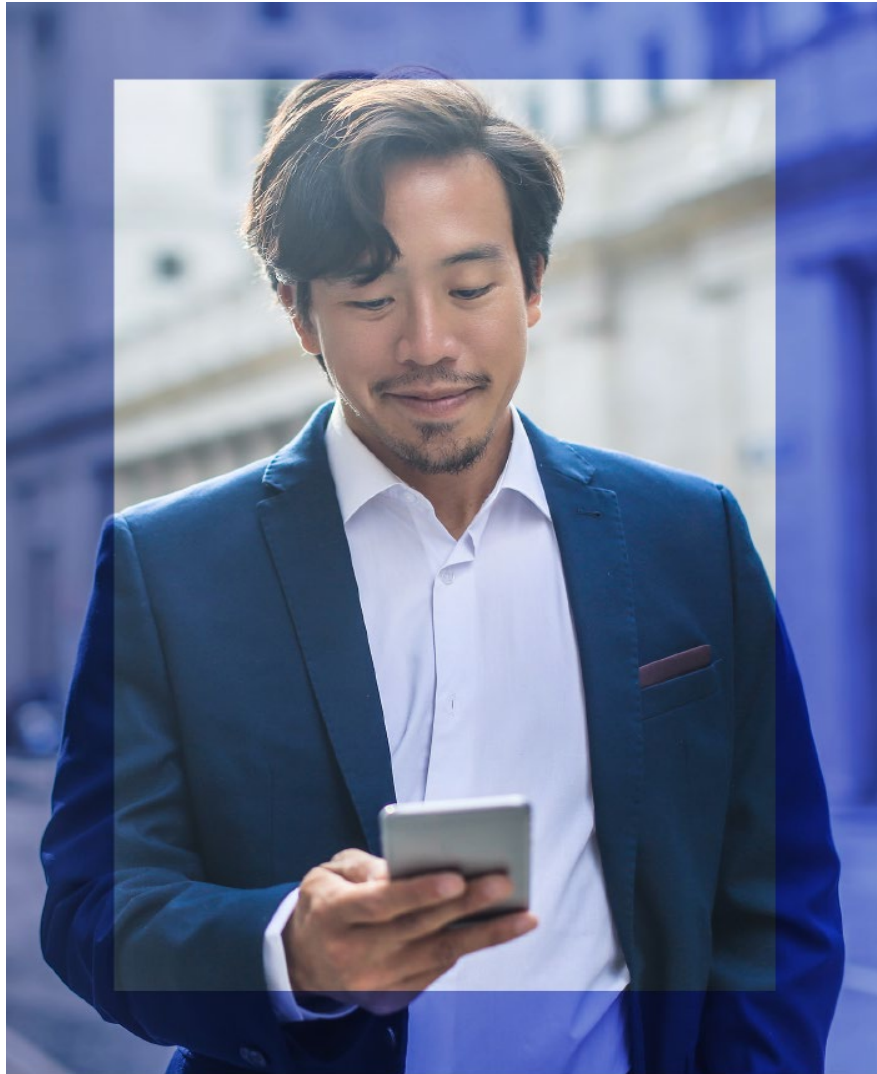
**Thomas Meyer**

Director – Cyber and Privacy at  
KPMG Belgium



**Dimitri Van Hoolst-  
Matthyssen**

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

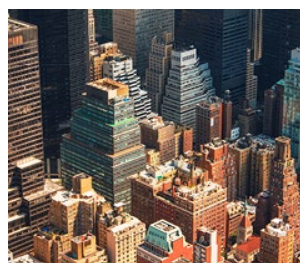
# DORA webinar series overview

Today



**Establishing a solid governance framework with ServiceNow**

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



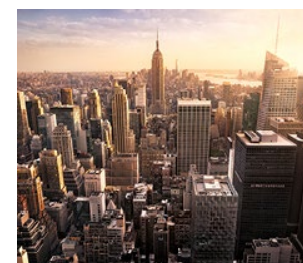
**Navigating the IT Risk landscape with ServiceNow**

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



**Streamlining third-party risk mgmt. with ServiceNow VRM**

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

# 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.



# Become a Trusted partner for your stakeholders

Perhaps the most fundamental shift in perspective is the understanding that a dynamic risk environment presents threats and challenges not just to the enterprise itself, but to all the stakeholders who have an interest in the organization.

This is what happens when you commit to earning and deserving the trust of all your stakeholders.



## Prepared

You develop the operational resilience and innovative agility to thrive through uncertainty.



## Informed

You are confident in your decision-making and clear about your direction for the future.



## Positive

You embrace risk and regulation as allies in the drive to grow and succeed in the right way.



## Respected

You are proud of the work you do, the leadership you provide and the example you set in the world.

# What is DORA?

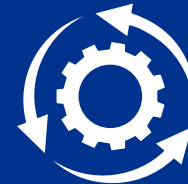
## Objectives

- A broader EU Digital Finance Package
- Fostering technological development
- Ensuring financial stability and consumer protection



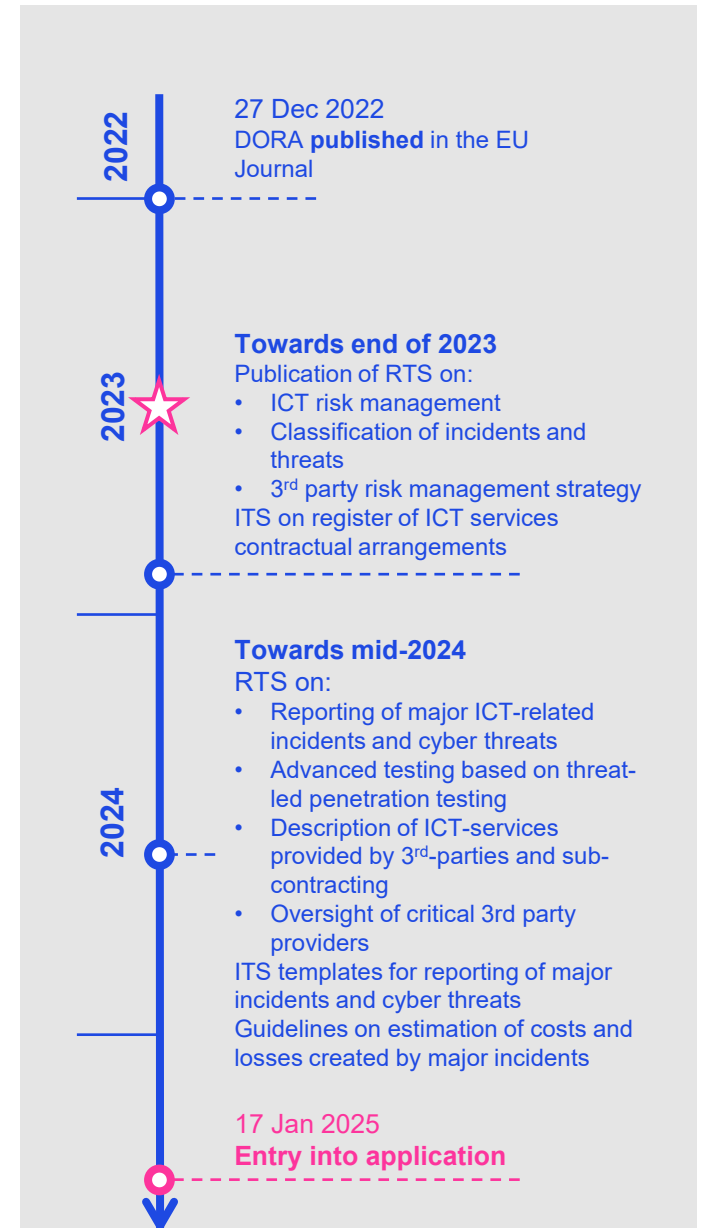
## Scope

- Harmonisation of rules
- Strengthening oversight
- Extending the regulatory perimeter



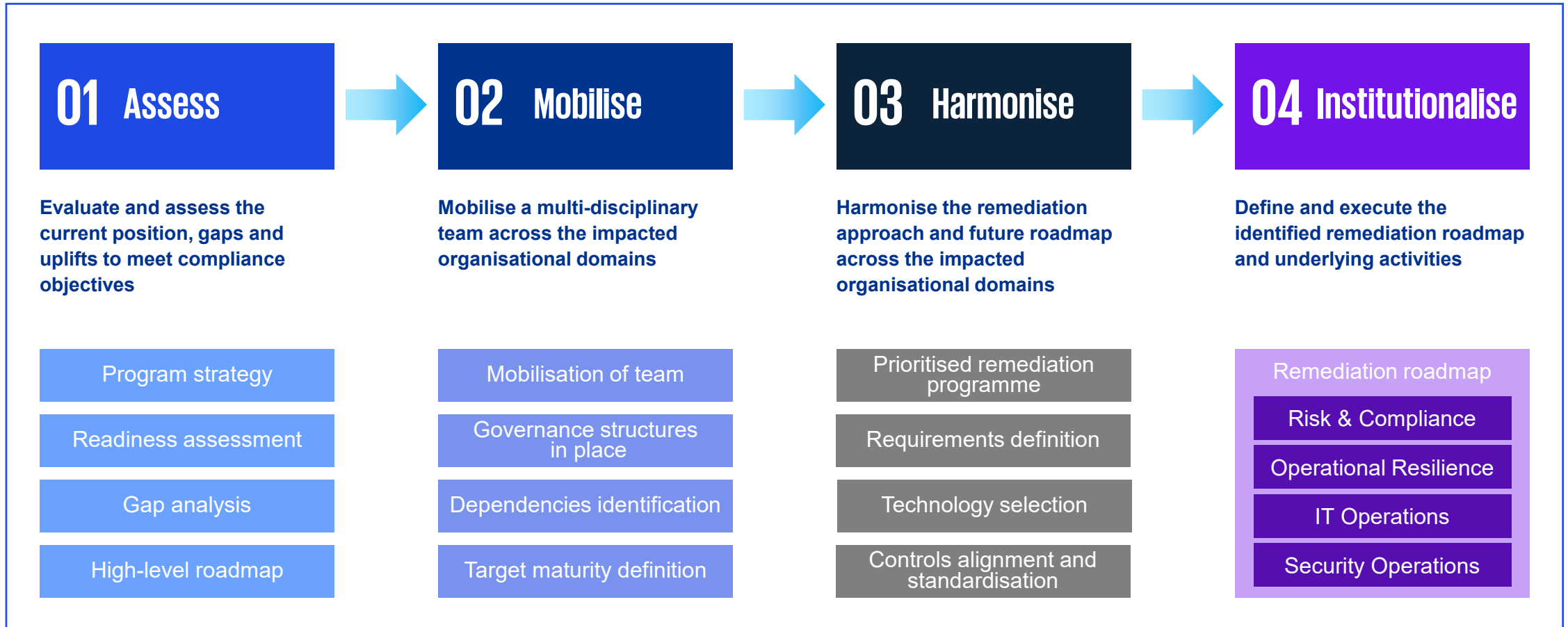
## Approach

- A European approach
- Legislative process



# The journey to DORA programme

A well-defined and governed process is needed to have a successful DORA programme within the timeframe given





# The six key areas of DORA

## Focus of today



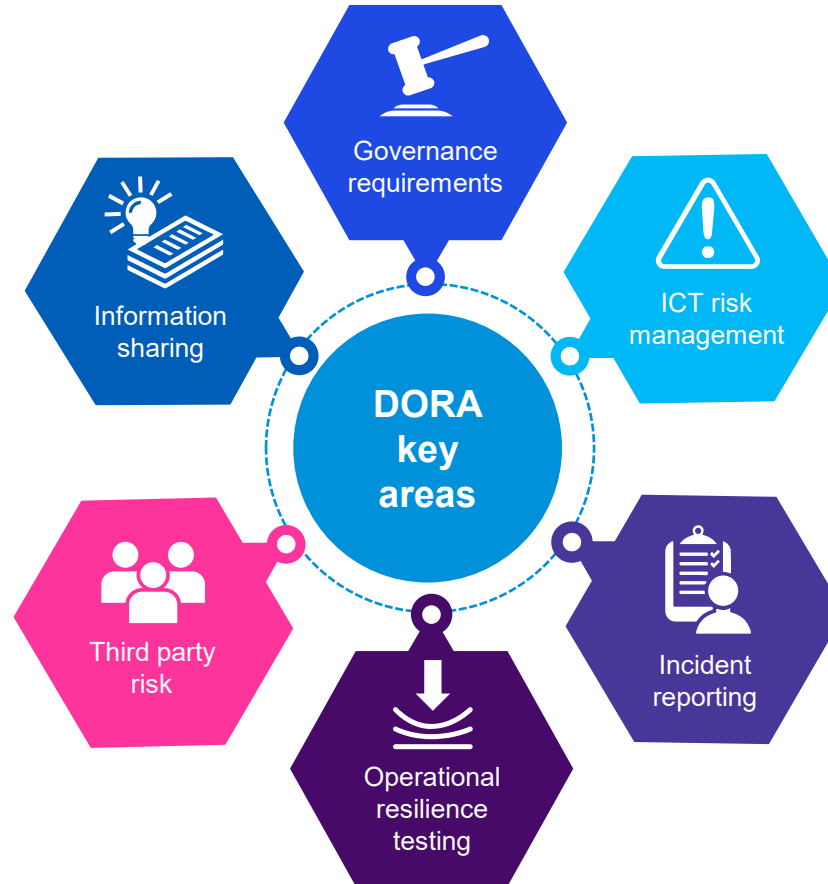
**Governance requirements**  
Internal controls and governance structure



**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

# DORA Governance in a nutshell

01

## Seeing the big picture

Have a holistic view that can inform senior management. Understanding the organisations role and importance in the marketplace. Provide proportionality over risk decisions.

02

## Putting the pieces together

Identify and sustain critical ICT functions and related assets, 3<sup>rd</sup> parties and dependencies. Ensure governance structures and polices are in place.

03

## Resilience starts within

Set clear ownership of your resilience strategy and incorporate in your day-to-day business. Provide employees with effective knowledge and understanding from the top to the bottom of the organisation

04

## Building resilience for better decisions

Report to support senior management decision making on the organisation's resilience position, and the threats and risk to it – alongside being able to report issues to regulators, customers, clients and other stakeholders

# Seeing the big picture

## Key Questions

- ✓ Do you understand your organizations role in the marketplace and how to apply proportionality to your risk decisions and appetite?
- ✓ Did you coordinate your operational resilience activities with your operational risk framework?
- ✓ Are your senior management teams equipped and sufficiently aware to make decisions on resiliency issues
- ✓ Are reporting lines clear and in the event of an incident can decisions be taken quickly to allow recovery and reporting within the timescales?

01

### Embedding your operational risk and control framework(s)

- Integrate and **embed your current risk and control frameworks to enhance preventive, response and recovery capabilities** to sustain your operational resilience
- **Incorporate the risks identified in your CIF mapping** with your service risk assessments
- **Understand your organisations position in the marketplace** to inform proportionality in the approach

02

### Provide organization-wide actionable data

- Set up **harmonized reporting** which will provide actionable data to the right stakeholders at the right time

03

### Embed in your future Target Operating Model (TOM)

- **Ensuring that senior management are equipped** with both the organizational structures, the information, people and skills to manage critical ICT events – may involve changing the model you have today
- Increased regulatory-driven approach – reporting to various third parties requires **management to have sufficient oversight and control over activities**

# Putting the pieces together

## Key Questions

- ✓ To what extent have you identified and ranked your most important business services?
- ✓ Are the critical ICT functions reviewed by the board and/or senior management?
- ✓ Are services mapped end-to-end, and top to bottom, and is a risk gap analysis performed?
- ✓ Are risks and gaps within appetited, and do appetite risks have a plan in place?

01

### Identify critical or important functions (CIFs)

- Agree on a **list of the most important services** provided by your organization that support your function in the marketplace and link these to your business and organizational strategy
- Use a **top-down approach**
- Understand the role third parties play in your ecosystem
- Consider impact on **external stakeholders** and **internal processes**

02

### Understand interdependencies

- **Map CIF business services** to supporting systems, facilities, people, third parties and data.
- Start with a **pilot** and go with multiple **iterations** for big organizations
- Perform a **risk assessment** based on **impact** on the critical function

03

### What do you need for the CIF to sustain

- **Validate resiliency plans** against reviewed risk appetite
- Link activities to **procurement and architecture** planning, strategy, and lifecycle
- **Third party exit** and contingency plans

04

### Conduct a fit-gap analysis

- **Are risks and gaps within appetite**, and out-of-appetite risks and gaps have remediation plans
- Understand how **third party risks need to be addressed**. May involve changes to contracts, exit plans, or migration strategies
- Ensure reporting, actions, budgets, and approvals have **senior management visibility**

# Resilience starts within

## Key Questions

- ✓ Does senior management feel well informed about the operational resilience activities in the organization?
- ✓ Do people at all levels have adequate training and understanding resilience and their role in supporting it?
- ✓ Are roles and responsibilities at all levels clearly documented, linked to policy and organizational structures?

01

### Set a tone from the top

- **Senior or top management is the owner of the operational resilience strategy** and should be involved in validating an organization-wide strategy
- Link these to your business and organizational strategy
- Use a **top-down approach**

02

### Define clear ownership

- **Have the business support your resilience framework**
- Define clear **roles and responsibilities** within your operational resilience framework
- Put in place **governance structures that re-enforce the roles, responsibilities, and accountabilities** for resilience and resilience risk

03

### Include resilience in your day-to-day business

- Set expectations on how to built in resilience in your **existing capabilities and activities**
- Make sure from senior management downwards, **people are clearly aware of their responsibilities**, and receive adequate training on resilience issues

# Building resilience for better decisions

## Key Questions

- ✓ Do you provide sufficient information to senior management to enable appropriate decision-making?
- ✓ Do your suppliers provide sufficient visibility to incorporate their risks into your processes?
- ✓ Are reporting formats, levels, and detail harmonized across the ICT risk landscape?
- ✓ Do you have adequate data to support rapid decision making by management during incident and regulatory reporting?

01

### Enable appropriate risk-based decision-making

- Monitor risks, vulnerabilities and issues outside the appetite to support senior level decision-making
- Provide holistic and harmonized view over ICT resilience risks in the organisation
- Ensure information is available to allow appropriate incident and regulatory reporting – includes regulators, clients, partners, and suppliers

02

### Set impact tolerances

- Understand role and importance of organisation in marketplace to adopt proportional approach
- Ensure harmonized approach across different risk types, and impact tolerances for events – both from a service, management, and reporting level

03

### Report on CIF level

- Reporting on CIF-level risks should form **part of normal governance and risk processes**
- Risk and issues should be able to be **linked to specific and relevant CIFs**
- **CIF issues should be available to stakeholders** for the CIF and senior management

# 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.



# Key areas of DORA mapped to ServiceNow

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



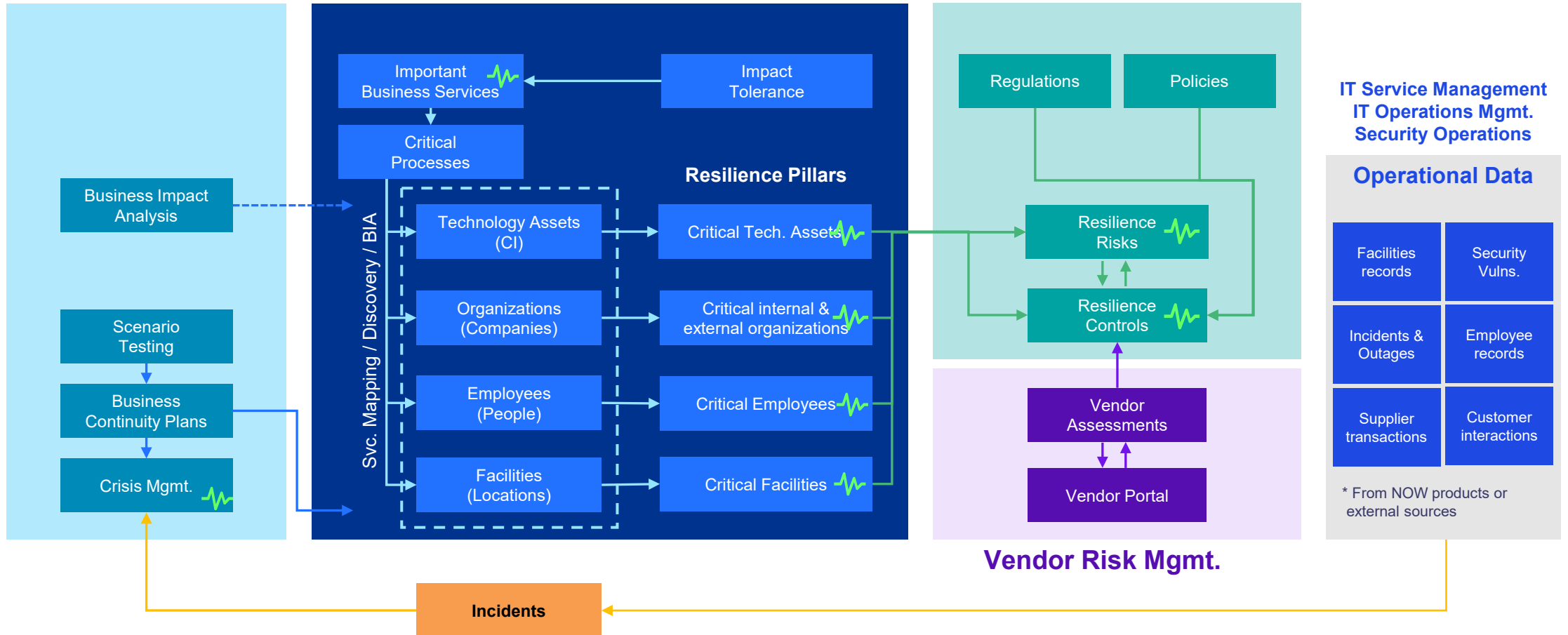


# The operational resilience workflow in ServiceNow

## Business Continuity

## Operational Resilience

## Integrated Risk Mgmt.



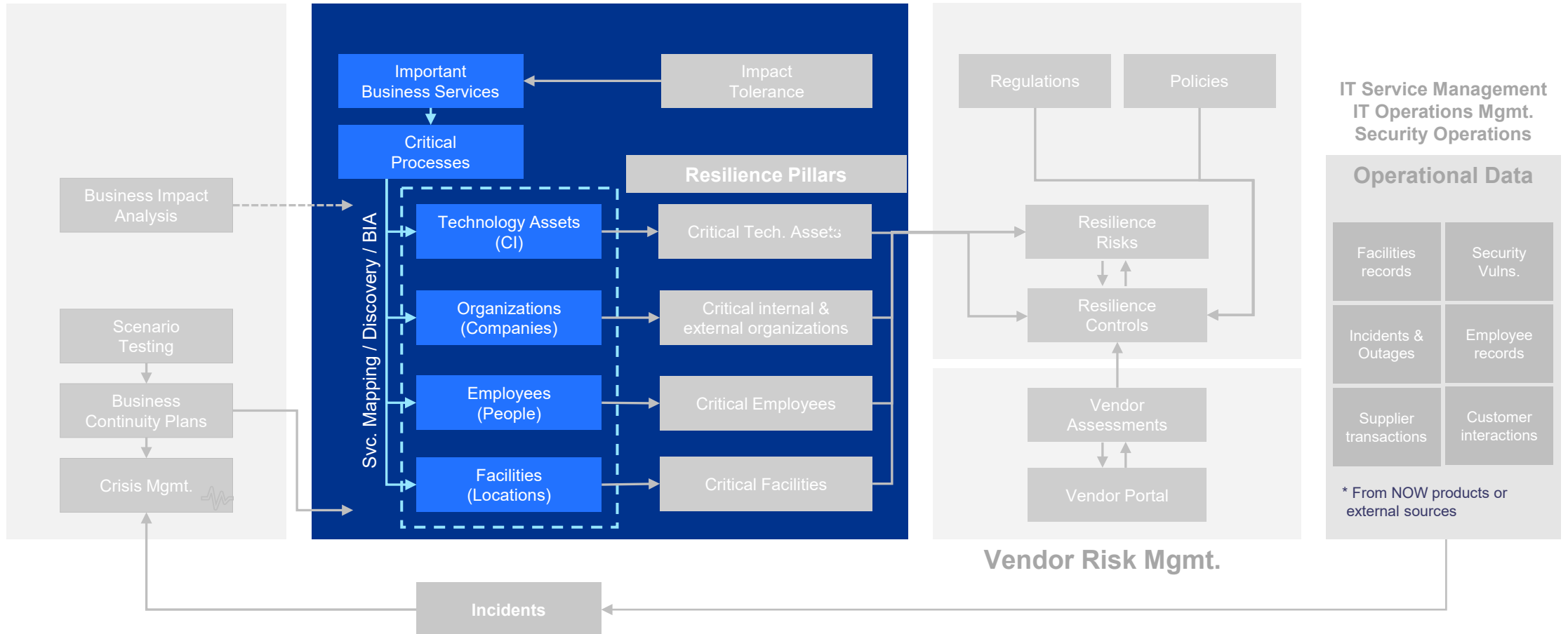
Operational Resilience Dashboards

# Setting up the governance structure (CIFs) in ServiceNow

## Business Continuity

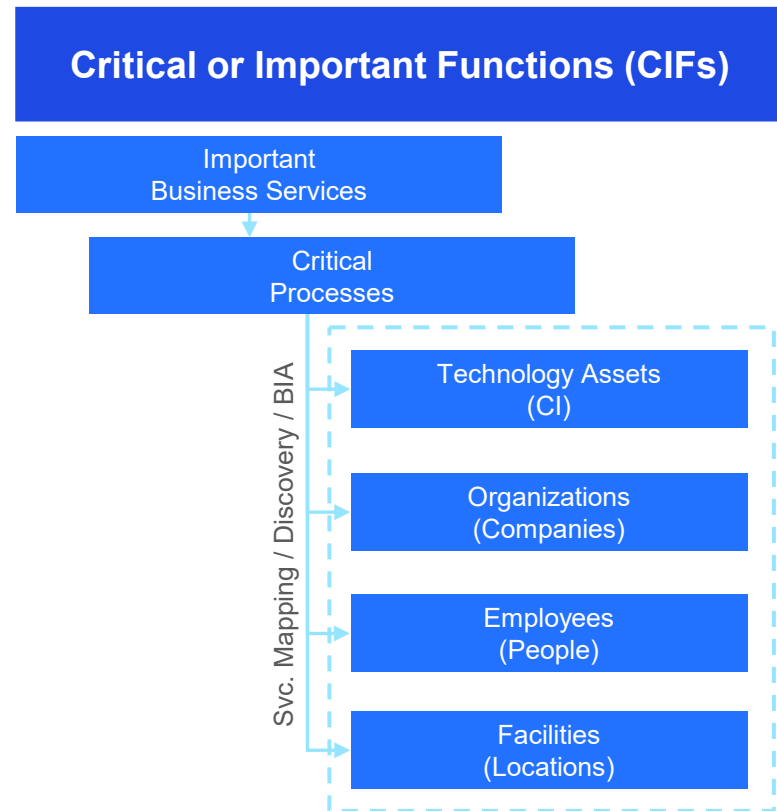
## Operational Resilience

## Integrated Risk Mgmt.

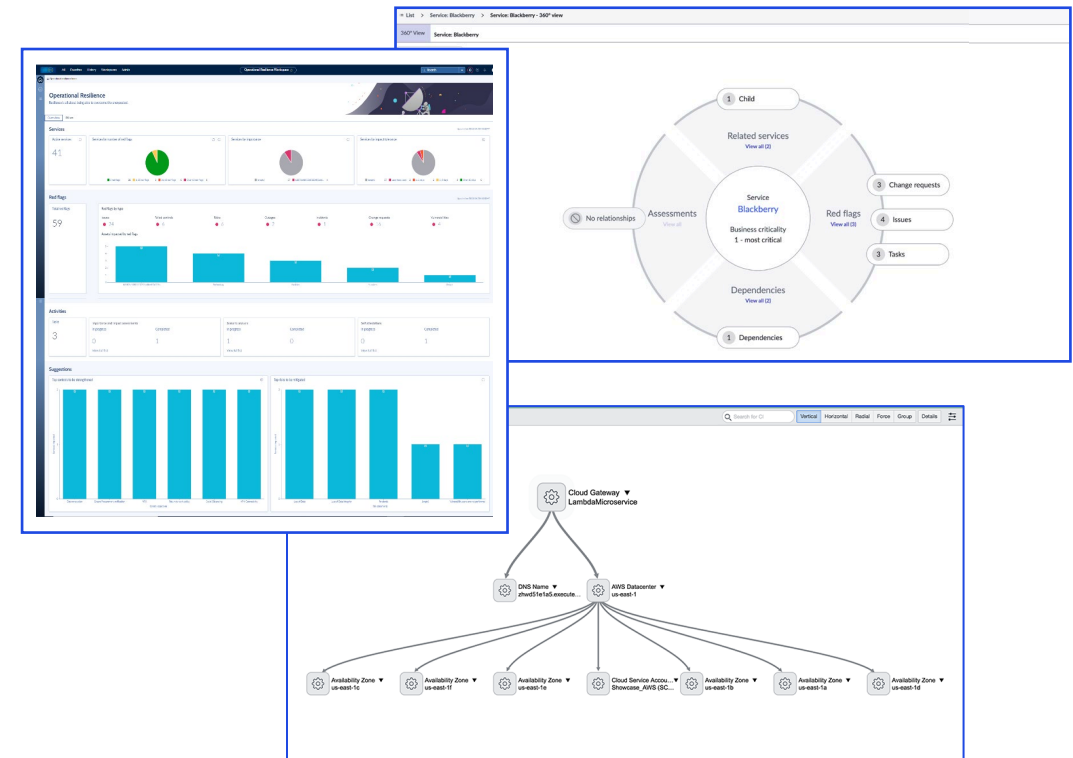


# Set up your CIFs as a base for DORA

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

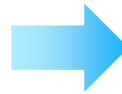
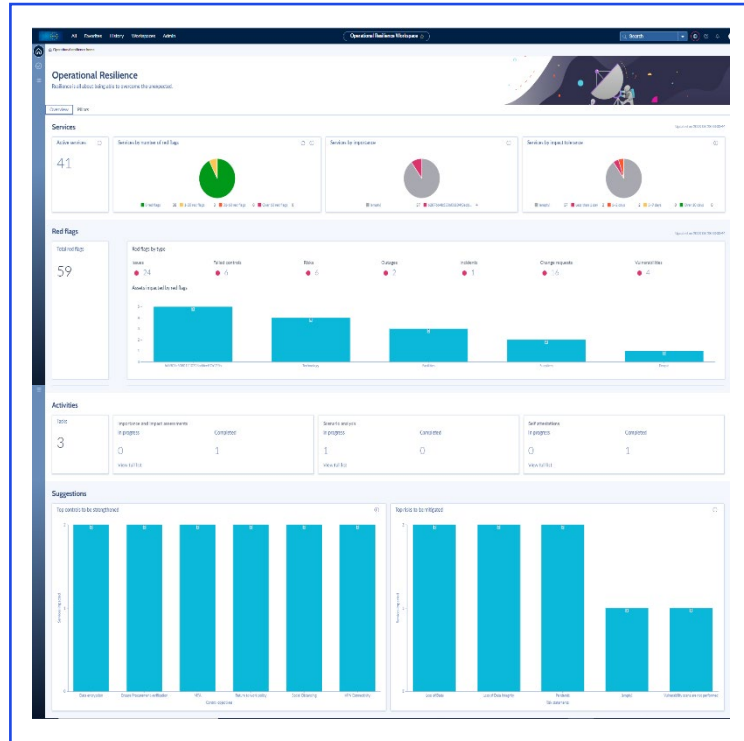


## Reporting



# ServiceNow demo – Operational Resilience

## Operational Resilience Workspace



## Service deep dive

Important Business Service:  
**Payments**



## Related objects



# 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

# Next webinars

## Next up



### Navigating the IT Risk landscape with ServiceNow

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



### Streamlining third-party risk mgmt. with ServiceNow VRM

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



### Establishing a solid governance framework with ServiceNow

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

### Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium

[thomasmeyer@kpmg.com](mailto:thomasmeyer@kpmg.com)

### Dimitri Van Hoolst-Matthysen

Manager – Solution Lead Powered Risk with ServiceNow at KPMG Belgium

[dvanhoolst@kpmg.com](mailto:dvanhoolst@kpmg.com)

### Hans Meulmeester

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

[hmeulmeester@kpmg.com](mailto:hmeulmeester@kpmg.com)

**KPMG**





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](https://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.

© 2023 KPMG Advisory, a Belgian BV/SRL and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

**Document Classification: KPMG Public**