



The journey of DORA

**Navigating the
IT Risk landscape
with ServiceNow**

DORA webinar series – 22/06/2023
KPMG Belgium

Presenters



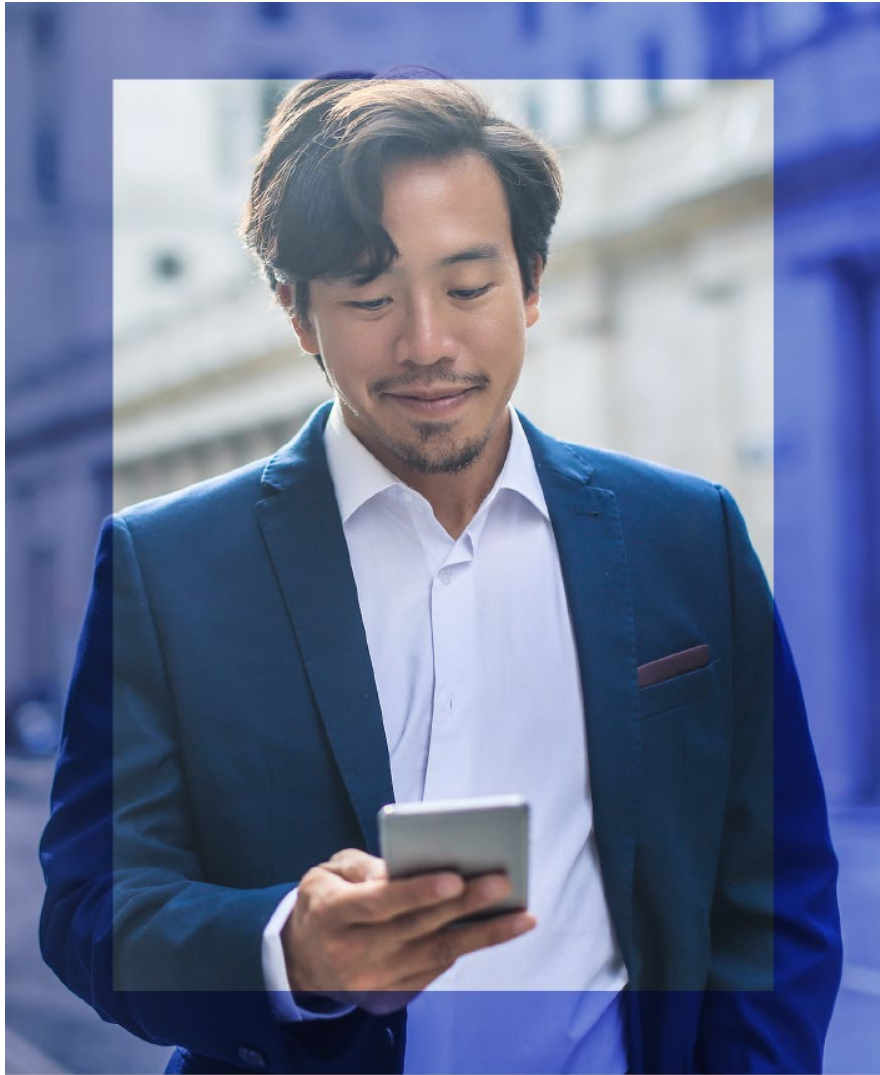
Thomas Meyer

Director – Cyber and Privacy at
KPMG Belgium



**Dimitri Van Hoolst-
Matthyssen**

Manager – Solution Lead
Powered Risk with
ServiceNow at KPMG Belgium

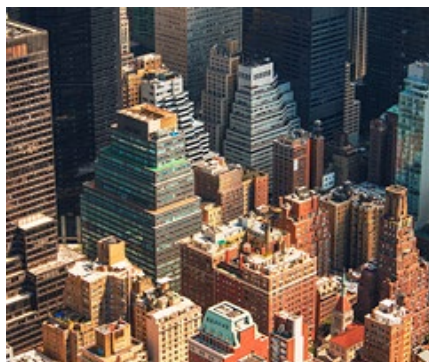


Contents

- 01** The journey of DORA
- 02** DORA ICT Risk Management area deep dive
- 03** Integrated Risk Management & ServiceNow
- 04** ServiceNow IRM demo
- 05** Recap and next topics

DORA webinar series overview

Today



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

The Journey of DORA – June Update

Latest developments

- Drafts released for consultation:
 - RTS on ICT risk management framework and RTS on simplified ICT risk management framework
 - RTS on criteria for the classification of ICT-related incidents
 - ITS to establish the templates for the register of information
 - RTS to specify the policy on ICT services performed by ICT third-party providers




Actions to be taken

- Identify if you wish to participate in feedback
- Incorporate RTS and ITS elements into your gap analysis
- Identify technologies and transformations
- Include related actions including technology deployment in DORA plan



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 ICT Risk Management in a nutshell

01

Setting clear boundaries

Setting up a risk appetite or tolerance will help you foster a risk-aware culture, enhance resilience, empower decision making and align risk management efforts with overall business.

02

Building a foundation

Integrating the critical functions (CIFs) to set up a comprehensive and holistic risk framework that covers all aspects of DORA and is embedded within the business

03

Fortifying your strategy

Integrate cyber and third party risk. Identify areas where rule-based approach will mean changes to existing approaches are needed.

04

Closing the loop

Harnessing outcomes of incidents, events gathered throughout the organization, alongside a review of risks and controls for continuous improvement of your risk management processes and framework.

RTS – High level structure for most organisations

Larger and more interconnected organisations



ICT security policies, procedures, protocols and tools (Article 15a)

Section I:
Provisions on
Governance

Section II:
ICT Risk
Management

Section III:
ICT Asset
Management

Section IV
Encryption and
Cryptography

Section V
ICT Operations
Security

Section VI:
Network Security

Section VII:
ICT Project and
Change Management

Section VIII:
Physical and
Environmental
Security

Section IX
ICT InfoSec
Awareness and
Training

RTS – High level structure for smaller organisations

Smaller and less interconnected organisations



Simplified ICT Risk Management Framework

**Chapter I:
ICT Risk Management
Framework**

**Chapter II:
Further Elements of
Systems Protocols, and
Tools to Minimise the
Impact of ICT Risk**

**Section III:
ICT Business Continuity
Management**

**Section IV
Report on the Review of the
ICT RMF**

Deep-dive on potential areas of challenge

01

Principles vs rules-based approach

- **Principle-based** – risk-based, flexible. Examples: ISO 27k, NIST CSF
- **Rules-based** – stringent criteria, defined control implementations. Examples: PCI-DSS
- **Hybrid** – flexible risk-management, targeted rules for areas attack and high-risk. Examples: DORA, SWIFT CSP
- Existing practices likely to need uplift, with review needed of current approach

02

Embedding resilience and security

- **Systems acquisition, development, and maintenance** – embedding security and resilience
- **Assets** – ICT and information
- **Performance and capacity** – more consistent approach, validation, and testing
- **Change and projects management** – embedding, testing, and confirmation of operation after change
- Uplift likely needed in project and change management to include additional items

03

Security Operations

- **Logging and monitoring** – focus area with details on what should be logged and monitored as well as rationale for approach
- **Vulnerability management** – tighter requirements on patching, proposed weekly scanning of all assets
- **System hardening** – further requirements to ensure this control is in place for in-scope assets
- **Encryption** – more defined processes
- Uplift in architecture, operating model, and technology possible

04

Reporting and integration

- **Integrated reporting**
- **Risk assessments** – required in multiple processes
- **3Lod/IA** – alignment needed as role of IA is key and required in determining compliance
- **PPPT** – Policies, procedures, protocols, and tools needed to embed across the various risk management areas
- More consistent embedding and reporting potentially needed
- Streamlining of risk assessment and management processes

“Financial entities should have a comprehensive and systematic approach to treating ICT risk...

...identified through the ICT risk assessment. By identifying and implementing appropriate measures and regularly monitoring their effectiveness, financial entities can mitigate and manage ICT risk in line with their risk tolerance levels. This contributes to the overall resilience and security of their ICT systems and operations.”

– DORA RTS on ICT risk management framework

Introduction to Integrated Risk Management (IRM)

IRM is a contested term, but at its heart is the idea that the key to effective risk management lies in the adoption of a set of common practices, frameworks, processes and enabling technologies which deliver genuinely holistic insights into an organization's risk profile and compliance status – thereby allowing organizations to make informed decisions, achieve their objectives and build trust with their stakeholders.

The KPMG Powered Enterprise | Risk offering can help play a key role in overcoming the challenges in achieving an integrated risk management implementation.

“

“An integrated approach which seeks to improve the breadth, depth and richness of an organization’s understanding of its risk profile - helping it to make decisions from an informed perspective, and thereby enabling it to reliably achieve its objectives, build trust with its stakeholders, and improve its performance.”

KPMG’s definition of IRM

Key areas of DORA mapped to ServiceNow

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

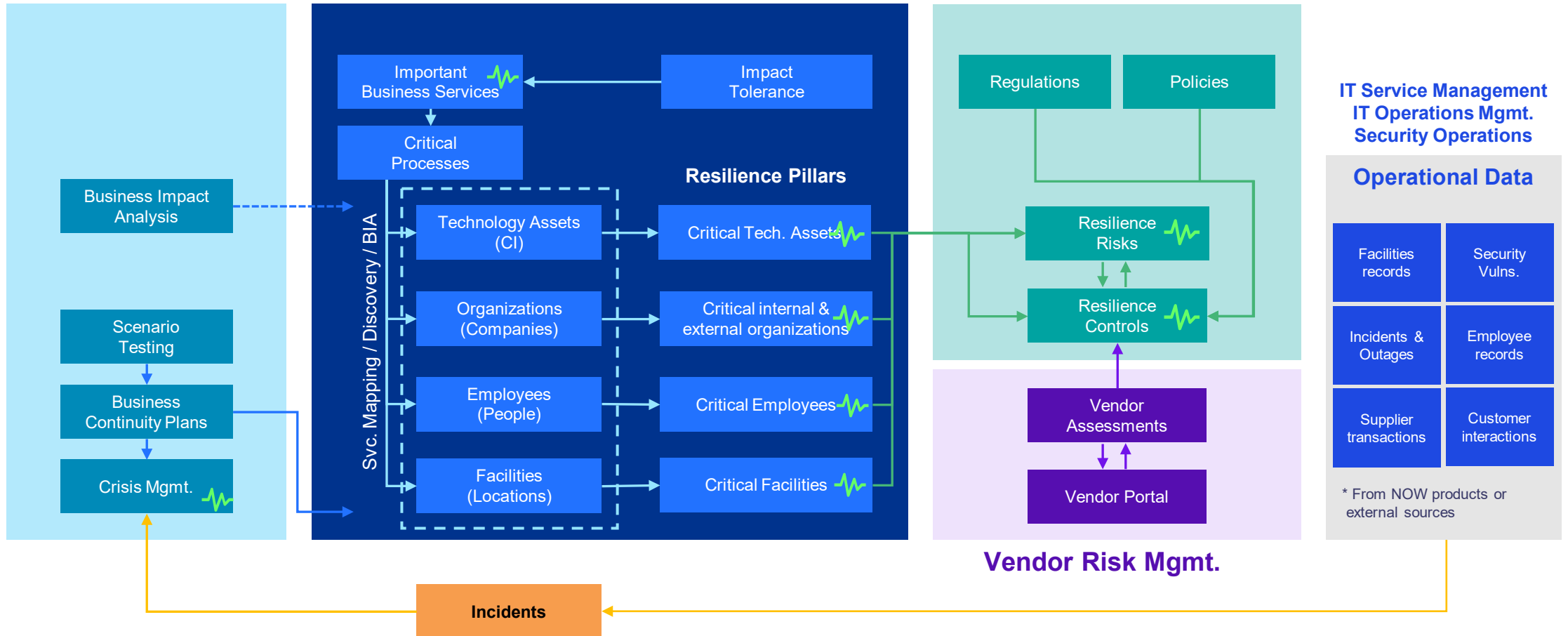


The operational resilience workflow in ServiceNow

Business Continuity

Operational Resilience

Integrated Risk Mgmt.

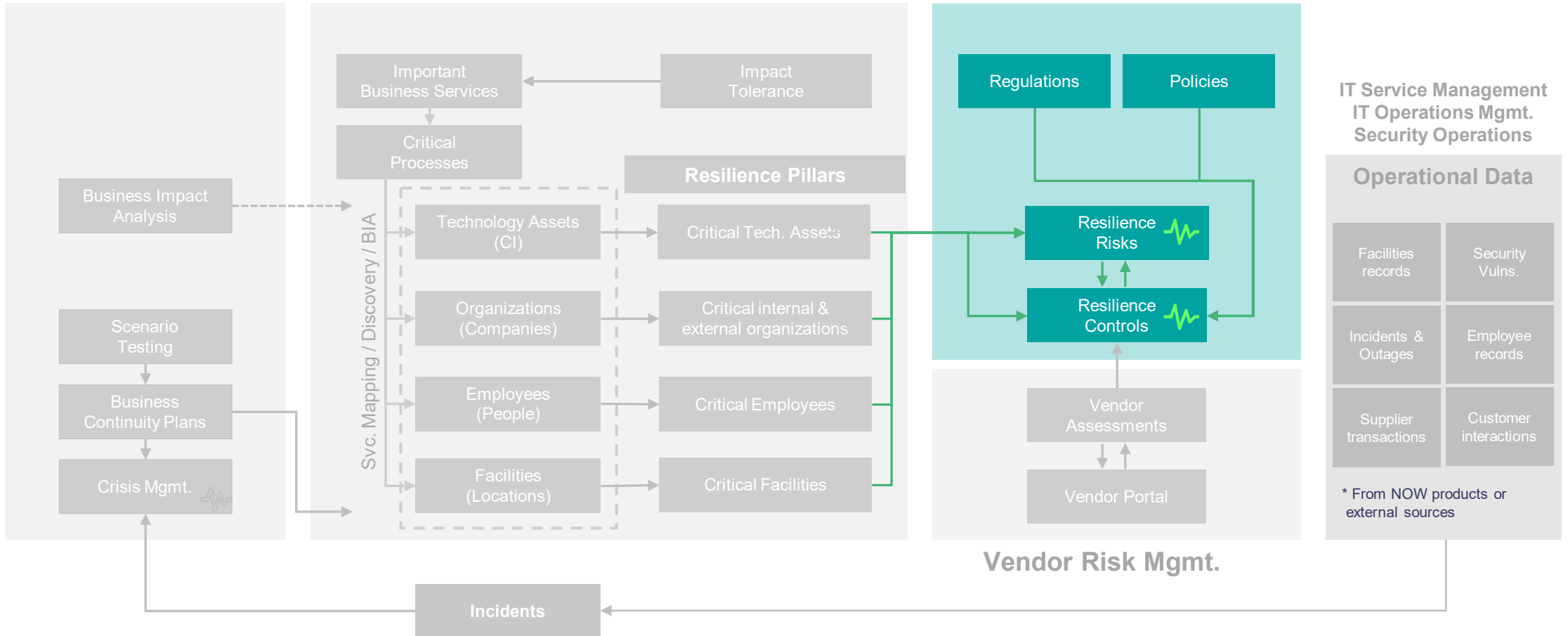


The operational resilience workflow in ServiceNow

Business Continuity

Operational Resilience

Integrated Risk Mgmt.



IT Service Management
IT Operations Mgmt.
Security Operations

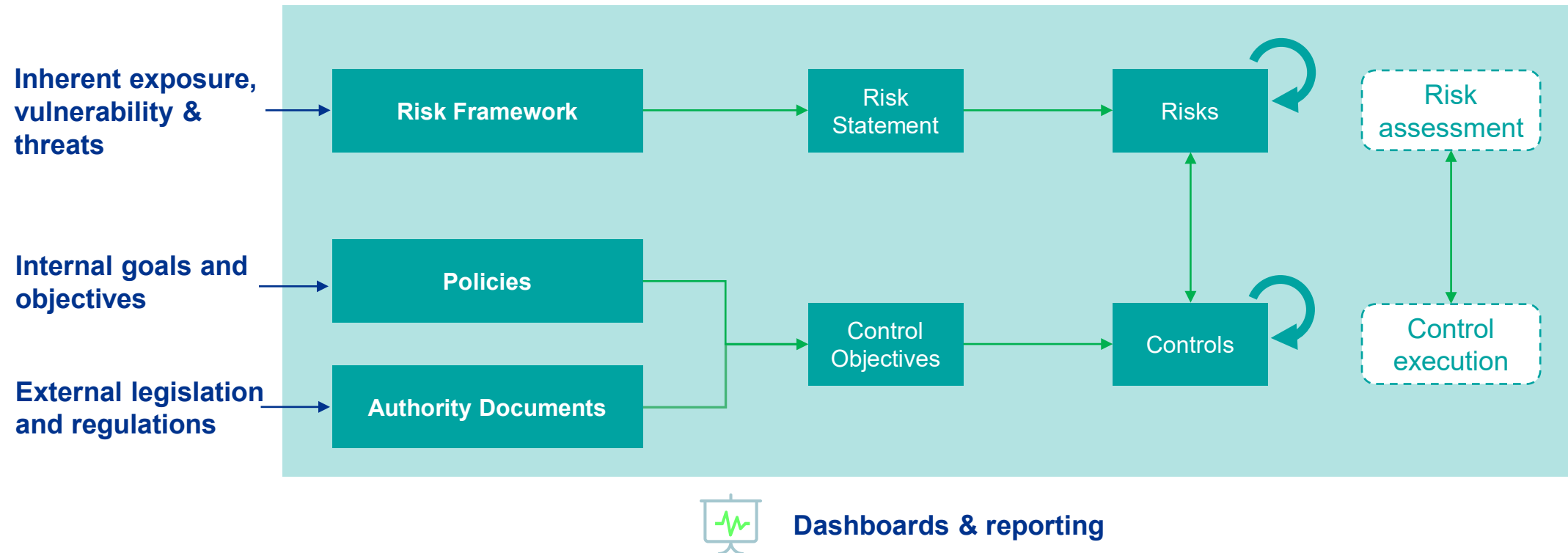
Operational Data

| | |
|-----------------------|-----------------------|
| Facilities records | Security Vulns. |
| Incidents & Outages | Employee records |
| Supplier transactions | Customer interactions |

* From NOW products or external sources

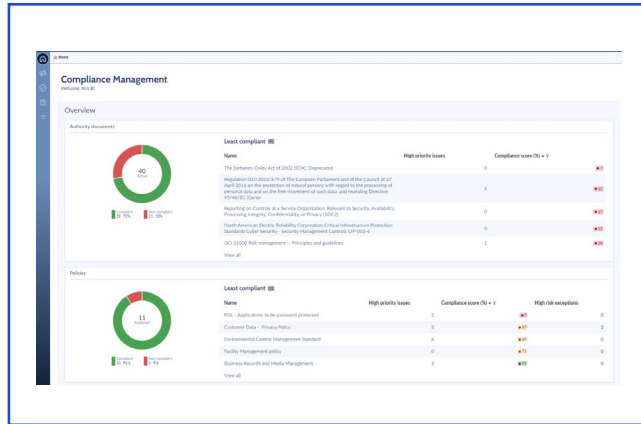
ServiceNow IRM enables you to efficiently demonstrate the risk and compliance levels of your organization

Integrated Risk Management

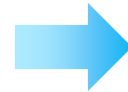
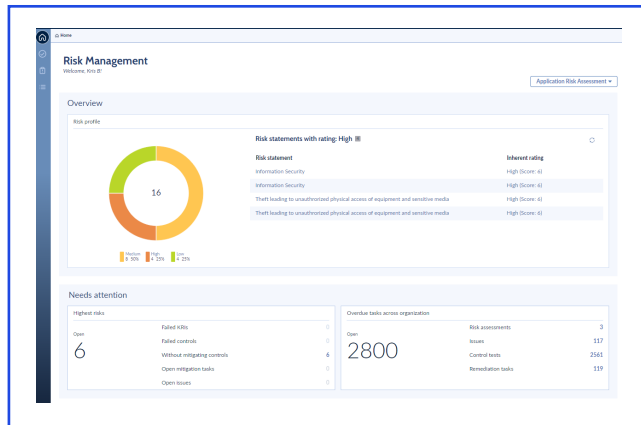


ServiceNow demo – Risk & Compliance Management

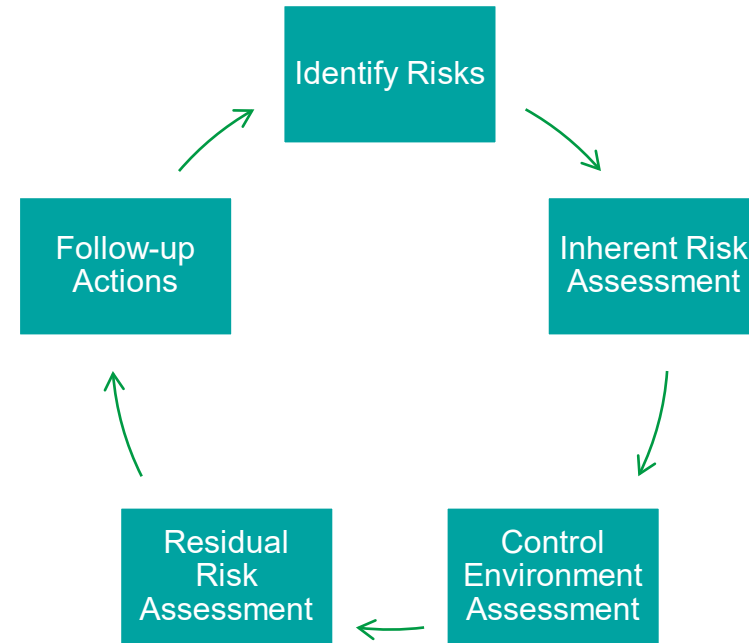
Compliance Workspace



Risk Workspace



Risk Assessment



Typical IRM transformation challenges

- 01.** | Clearly define the ambitions and desired level of maturity – Harmonize the processes and way of working across the organization
- 02.** | Make sure to involve all 3 lines of defense in the definition of the ambition and the end-to-end process
- 03.** | Identify at the start which technology can support your process, and try to stick to the standard
- 04.** | Start with a pilot process and/or team, and gradually rollout further across the organization
- 05.** | Change management is key to ensure the adoption of the new way of working by the teams in your organization

Next webinars

Next up



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



Navigating the IT Risk landscape with ServiceNow

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

Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium

thomasmeyer@kpmg.com

Dimitri Van Hoolst-Matthysen

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

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

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