KPMG

The journey of DORA

Powering your compliance with Security Operations

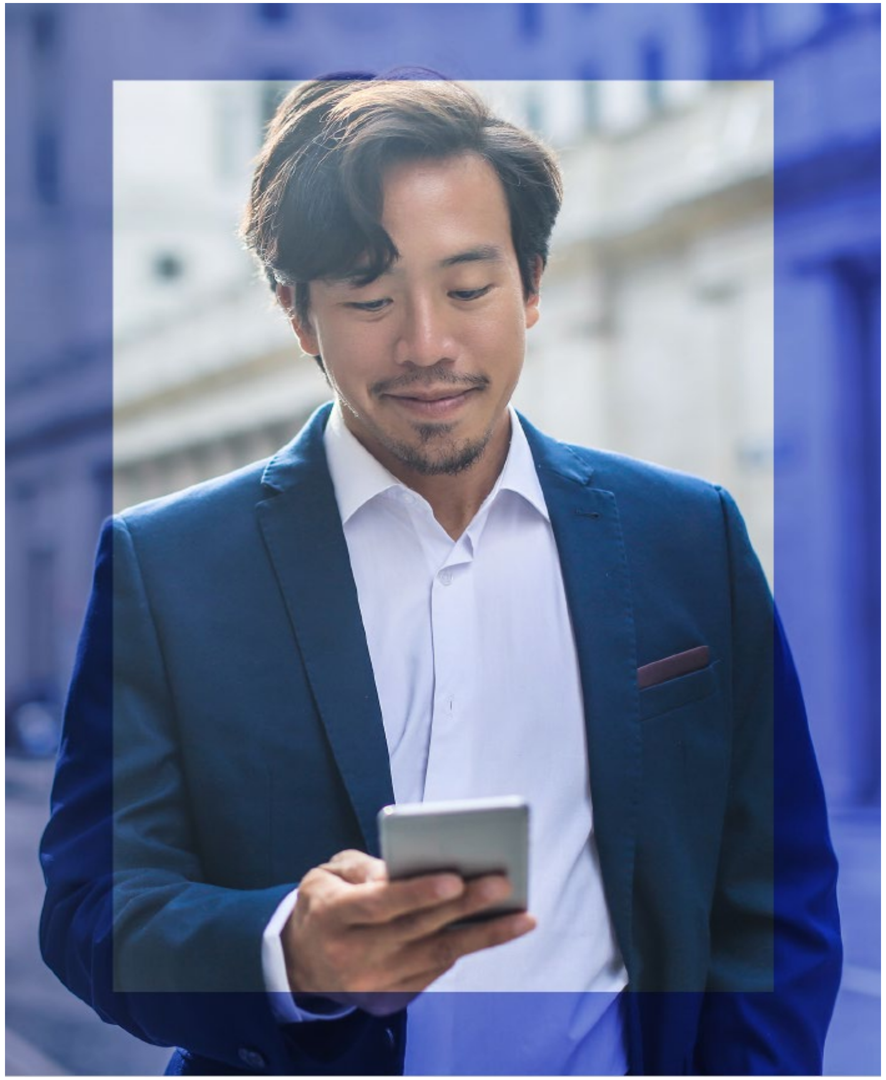
DORA webinar series – 23/11/2023
KPMG Belgium

Presenters

Thomas Meyer

Director – Cyber and Privacy at KPMG Belgium

thomasmeyer@kpmg.com



Contents

01 The journey of DORA

02 DORA & Incident reporting deep dive

03 Security Operations in ServiceNow

04 Next steps

DORA webinar series overview

Today

Powering your compliance with Security operations

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

01

The journey of DORA

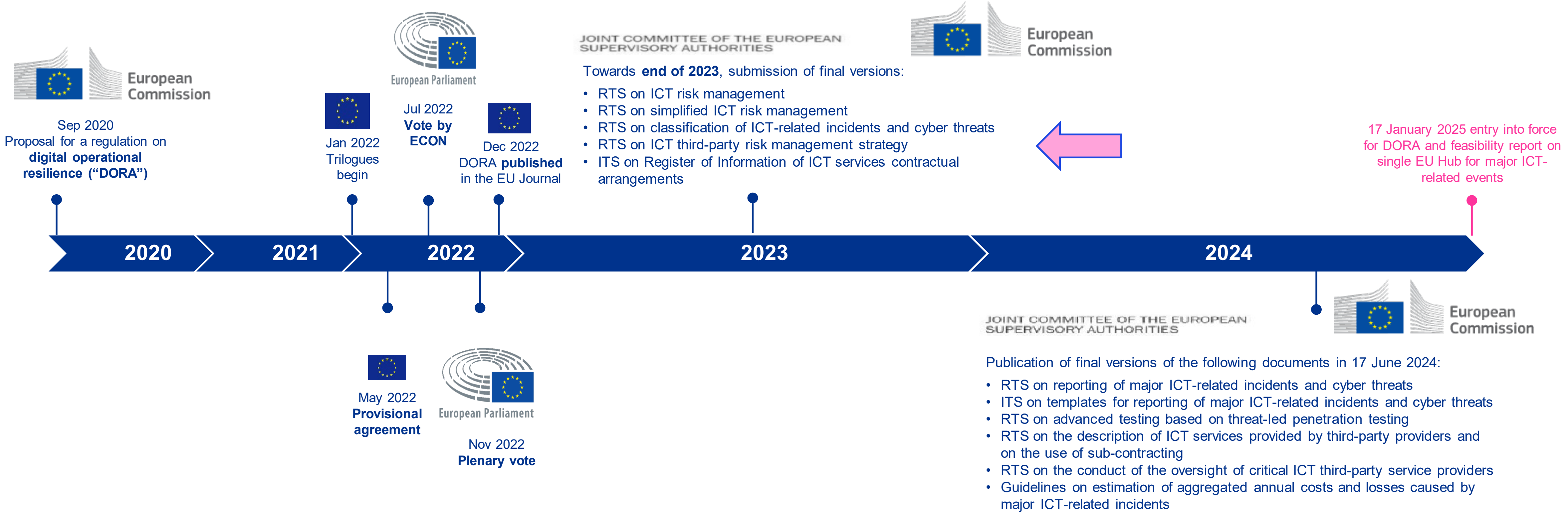
DORA is not a “one-off” compliance exercise, but will push you to get and remain resilient.

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**, submission of final versions:

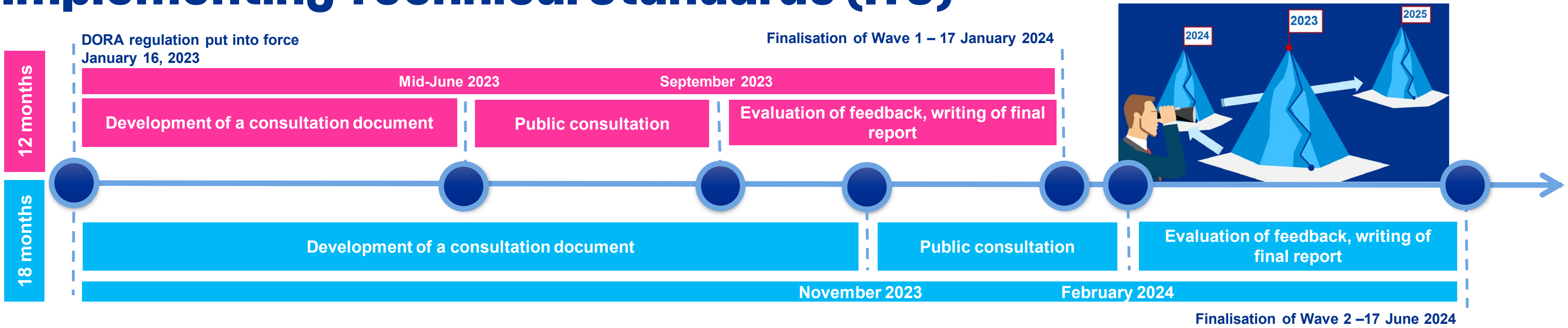
- RTS on ICT risk management
- RTS on simplified ICT risk management
- RTS on classification of ICT-related incidents and cyber threats
- RTS on ICT third-party risk management strategy
- ITS on Register of Information of ICT services contractual arrangements

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

Mid-June 2023

September 2023

Finalisation of Wave 1 – 17 January 2024

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 – incident reporting & information-sharing

The six key areas of DORA

Governance requirements

Internal controls and governance structure

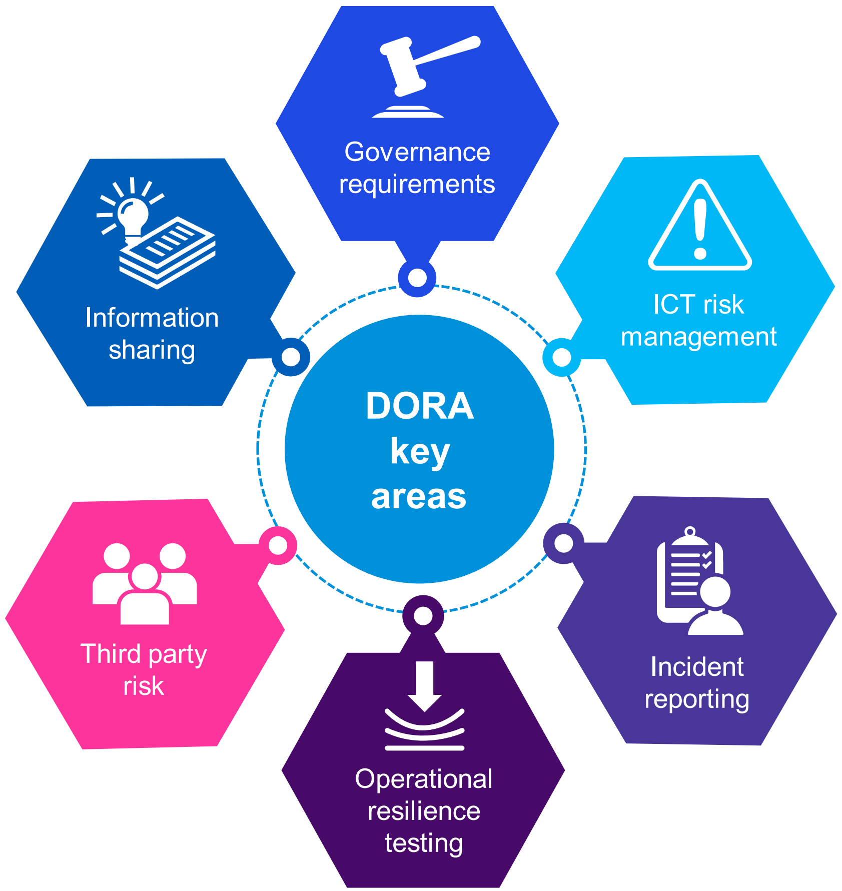
Focus of today

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

Focus of today

Incident reporting

Reporting thresholds and systems to communicate to regulators and users

Operational resilience testing

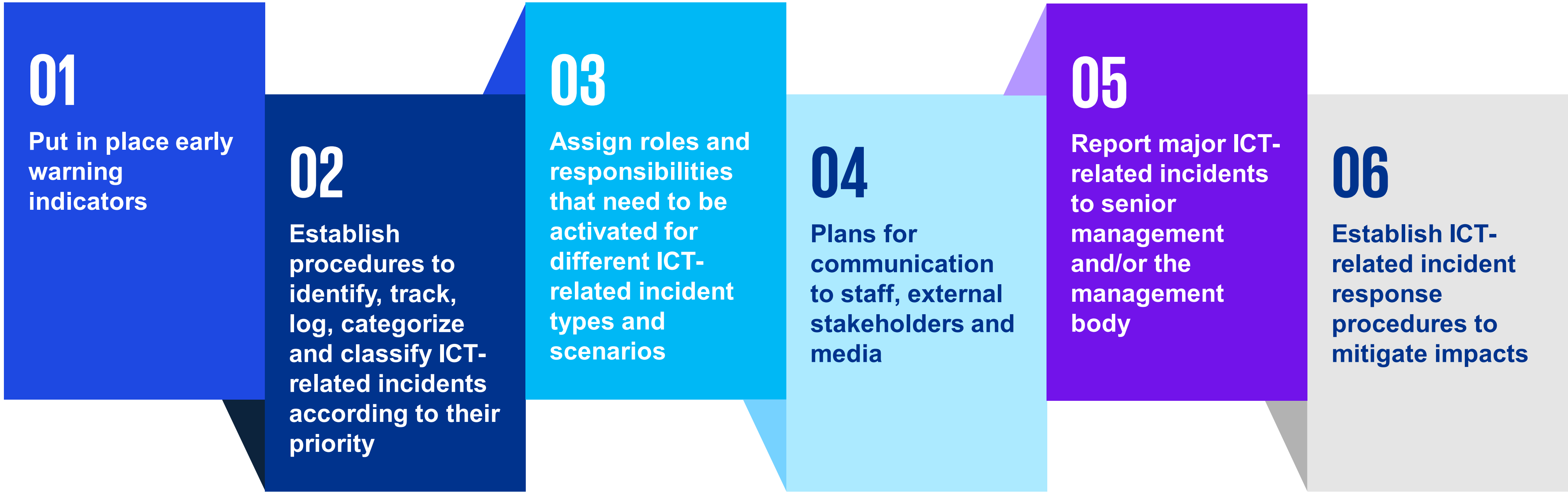
Testing for preparedness and weakness identification

Goals, approach and observations

- **Harmonisation** – across legislation and provide consistency across member states
- **Efficiency and** proportionality – materiality thresholds designed to exclude smaller institutions unless a significant incident
- **Encourage information sharing**
- **PSD2 alignment is not complete** – more systems and process in-scope and some organisations have stricter provisions. Organisations with detailed PSD2 reporting capabilities will be well placed to adapt
- **Coordinated approach** – IT, Cyber, TPRM, Compliance, Legal, and others will need to align processes
- **Data** – many aspects require rapid access to accurate data and figures on business and IT impacts, and associated costs
- **Contains:**
  - Incident process
  - Classification and materiality
  - Notification process
  - Information sharing requirements and approach
- **17th January 2024 – next batch of RTS and ITS for consultation, including reporting templates. Final versions of the RTS on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554**

ICT-related incident management process

Establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents



01 Put in place early warning indicators

02 Establish procedures to identify, track, log, categorize and classify ICT-related incidents according to their priority

03 Assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios

04 Plans for communication to staff, external stakeholders and media

05 Report major ICT-related incidents to senior management and/or the management body

06 Establish ICT-related incident response procedures to mitigate impacts

Major incident criteria, materiality and classification

Major Incident

2+ Primary

1 Primary

2+ Secondary

- Clients, financial counterparts, and transactions
- Data loss
- Critical services affected
- Reputational Impact
- Duration and service downtime
- Geographical spread
- Economic impact

Recurring

Meets criteria for major incident when incidents are aggregated over a 3 month period – incident must be similar in nature and impact

Primary criteria and materiality

01

Clients, financial counterparts and transactions

- **Number of clients**: **>10% or +50k**; or
- **Number of financial counterparties** that have contractual relationship: **>10%**; or
- **Transactions**: **10%** of regular level or +€15m
- **Business objective or market efficency**: Yes/No
- **Consideration**: one part of transaction must be in EU; estimates from similar periods can be used
- **Observation**: estimates can be a stand in, but we recommend developing more automated means to determine impact

02

Data loss

- Any impact on business objectives, or meeting regulatory requirements taking into consideration the below
- CIA – **AAIC** (newcomer is Authenticity)
- **Availability** – data has been made inaccessible to unusable to client/counterparties also considering market impact
- **Authenticity** – compromise of trustworthiness or reliability of data
- **Integrity** – unauthorised modification of data such that it is inaccurate or incomplete.
- **Confidentiality** – data that is accessed by or disclosed to unauthorised parties.
- **Observation**: GDPR and many existing process can support this.

03

Critical services affected

- **Scope** – includes transactions and operations
- **Assess** –have services or activities that require authorisation, or ICT services that CIFs been impacted
- **Observation**: Clear links with third party risk management are key to accurate and timely reporting beyond IT Service and Cyber incident reporting

Secondary criteria and materiality

01

Reputational impact

- Visibility – attracted media attention, receiving complaints, has or may breach regulations, loss of business with impact on business objectives
- **Observation:** Requires greater collaboration between marketing, compliance, business, and ICT functions.

02

Duration and service downtime

- **Downtime** – fully or partially unavailable to clients and counterparties compared to level of service before
- **Delays in provision of service** – if this occurs, the incident is not considered resolved until the delayed service is provided
- **Incident duration** – longer than 24hrs
- **ICT services supporting CIFs** – stricter requirements may be needed

03

Geographical spread

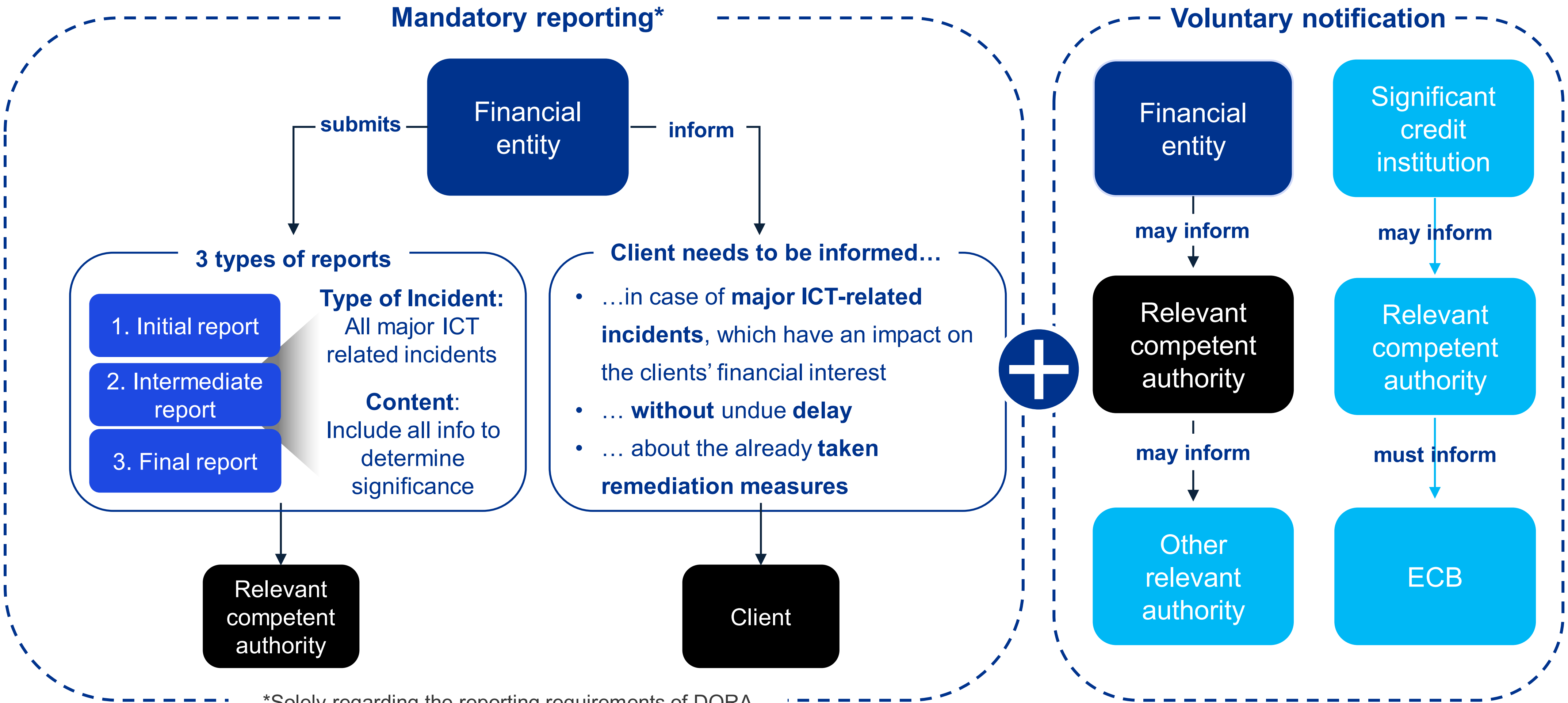
- **Focus** – impact to other jurisdictions
- **Impact** – more than one member state. **Other factors –**
- impact on clients and counterparties
- Other branches or financial entities in the group in another member states
- FMIs or third party providers that may be in common with other financial entities
- **Observation**: group entities will need to establish clear lines of communication to support incident activity

04

Economic impact

- **Direct + indirect gross costs and losses have or are likely to exceed €100000**
- Expropriated funds or financial assets
- Replacement or relocation costs of ICT items
- Staff costs
- Fees due to non-compliance with contractual obligations
- Customer compensation
- Loses due to forgone revenues
- Costs for internal and external communication
- **Advisor costs** – legal, forensic, advisory, remediation services
- **Note**: Not BAU costs and estimates can be used

Mandatory and voluntary reporting



Mandatory reporting*

Financial entity

submits

inform

3 types of reports

1. Initial report
2. Intermediate report
3. Final report

Type of Incident: All major ICT related incidents

Content: Include all info to determine significance

Relevant competent authority

Client needs to be informed…

- …in case of **major ICT-related incidents**, which have an impact on the clients' financial interest
- … **without** undue **delay**
- … about the already **taken remediation measures**

Client

Voluntary notification

Financial entity

may inform

Relevant competent authority

may inform

Other relevant authority

Significant credit institution

may inform

Relevant competent authority

must inform

ECB

*Solely regarding the reporting requirements of DORA

Voluntary cyber threat reporting

01

Classification

- **Significance** – based on:
  - Criticality of the services at risk – transactions and operations, and CIFs
  - Number and/or relevance of clients or financial counterparties targeted where high probably of materialisation
  - Geographical spread
- **Assessing probability** – includes
  - Applicable risks – related to the cyber threat including potential vulnerabilities – important link to TPRM
  - Capabilities and intent of threat actors
  - Persistence of the threat and knowledge about incidents impacting others or received from information-sharing sources

02

Data loss

- Any impact on business objectives, or meeting regulatory requirements taking into consideration the below
- CIA – **AAIC** (newcomer is Authenticity)
- **Availability** – data has been made inaccessible to unusable to client/counterparties also considering market impact
- **Authenticity** – compromise of trustworthiness or reliability of data
- **Integrity** – unauthorised modification of data such that it is inaccurate or incomplete.
- **Confidentiality** – data that is accessed by or disclosed to unauthorised parties.
- **Observation**: GDPR and many existing process can support this.

03

Critical services affected

- **Scope** – includes transactions and operations
- **Assess** –have services or activities that require authorisation, or ICT services that CIFs been impacted
- **Observation**: Clear links with third party risk management are key to accurate and timely reporting beyond IT Service and Cyber incident reporting

Information sharing

Financial entities are encouraged to exchange information to increase the overall cyber security of companies.

01 GOAL OF THE EXCHANGE

The objectives of the information exchange are:

- Raise awareness of ICT risks and minimise their propagation
- Support defence capabilities and threat detection techniques

02 REPORTING AUTHORITIES

Notification of the competent authorities:

- Confirmation of participation in agreements
- Begin of termination of participation

03 AGREEMENTS

- Strengthening digital operational resilience
- Within a trusted community
- Maintaining trade secrecy
- Protection of personal data
- Adherence to competition policy guidelines

04 TYPE OF INFORMATION

- Cyber threat information
- Indicators of compromise
- Tactics, techniques, and procedures
- Cyber security alerts and configuration tools

DORA Incident reporting in a nutshell

01 Develop a coordinated approach for your incident process across teams, processes and group entities that can operate in a timely fashion

02 Identify tooling, data sources and monitoring needed – both current and future – this should include model that may be used for estimates

03 Ensure processes are tested and can operate at the level needed

04 Evaluate potential use of information-sharing in ICT incident-related processes

03

SecOps & 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

Focus of today

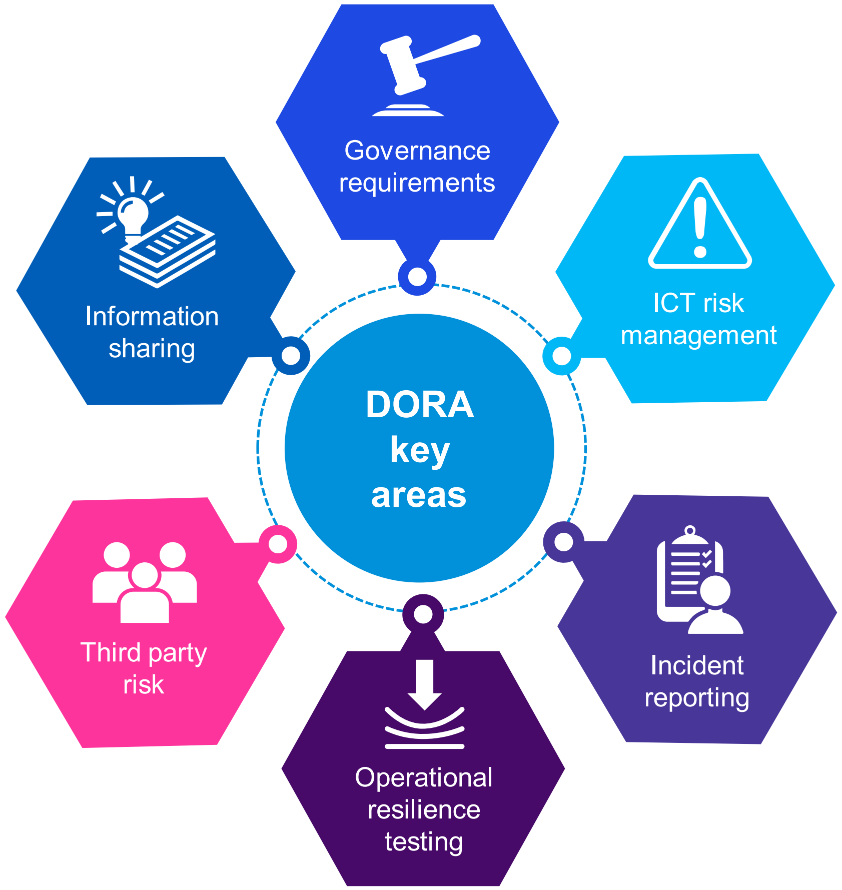
Information sharing

- **SecOps** (Security Operations)

VRM

Third party risk

- **VRM** (Vendor Risk Management)



ICT risk management

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

IRM

BCM

Focus of today

Incident reporting

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

ITSM

SecOps

IRM

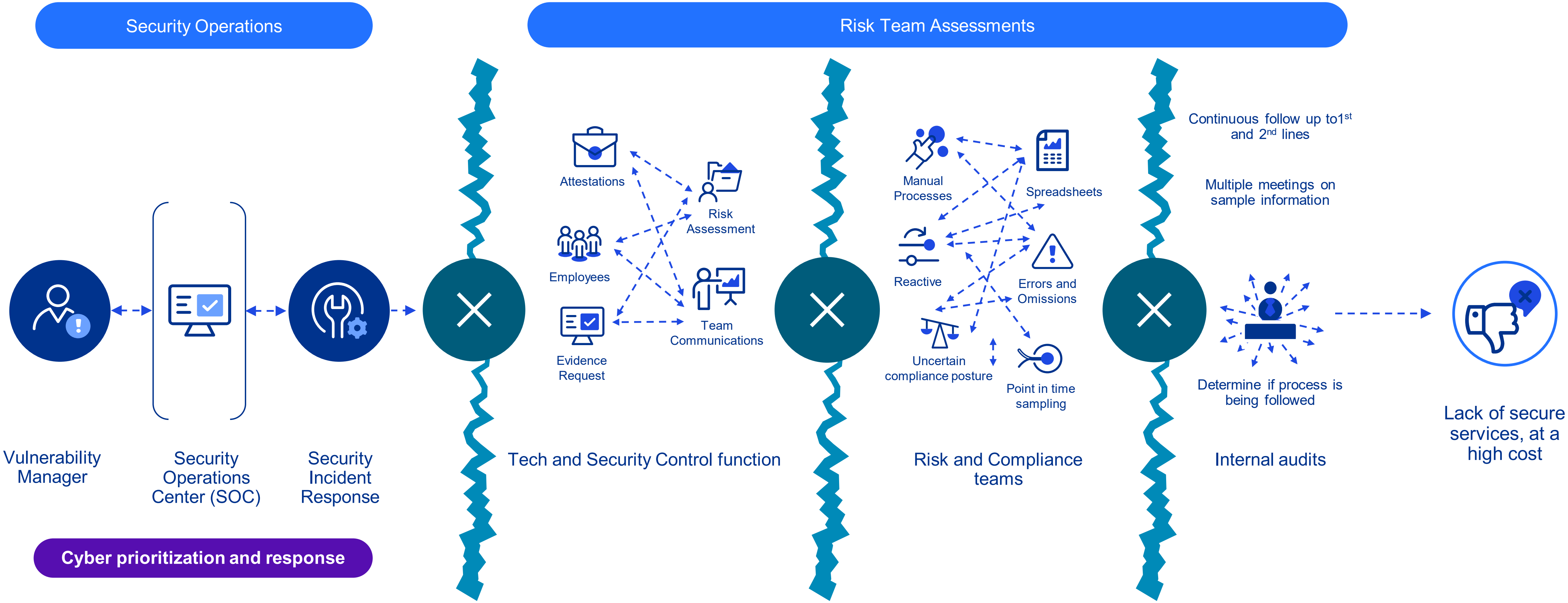
Operational resilience testing

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

Ops. Res.

BCM

Disconnected technologies and teams create ineffective and costly security and risk management



Security Operations

Risk Team Assessments

Vulnerability Manager

Security Operations Center (SOC)

Security Incident Response

Cyber prioritization and response

Attestations

Risk Assessment

Employees

Team Communications

Evidence Request

Tech and Security Control function

Manual Processes

Spreadsheets

Reactive

Errors and Omissions

Uncertain compliance posture

Point in time sampling

Risk and Compliance teams

Continuous follow up to1st and 2nd lines

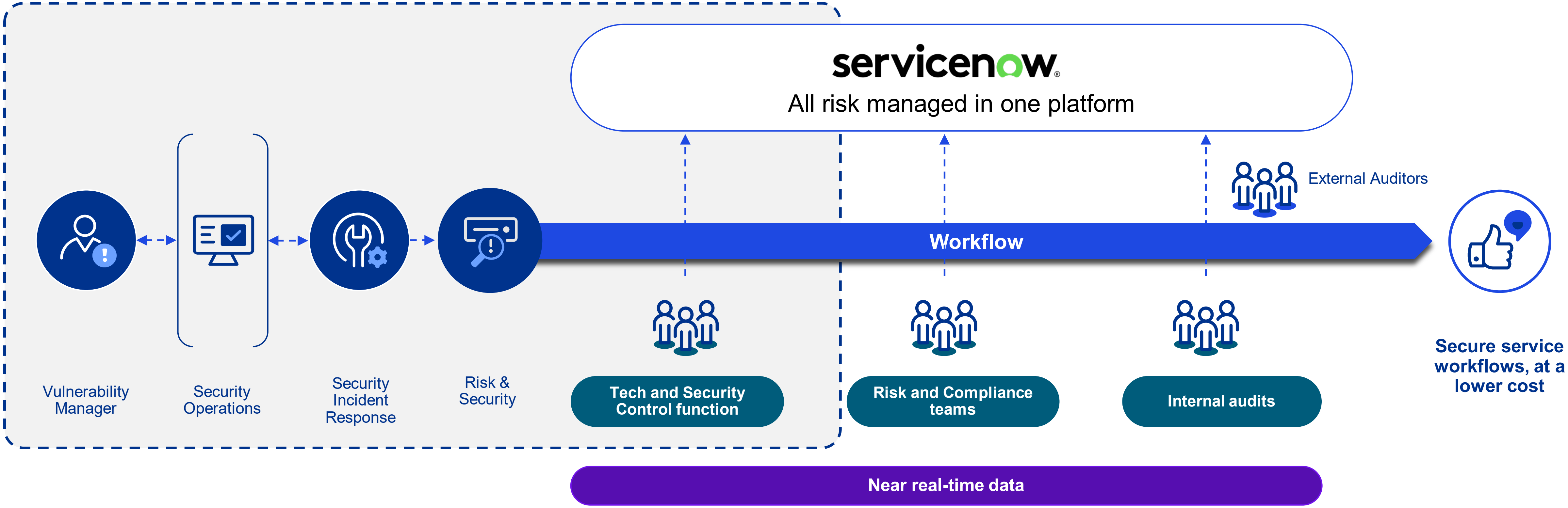
Multiple meetings on sample information

Determine if process is being followed

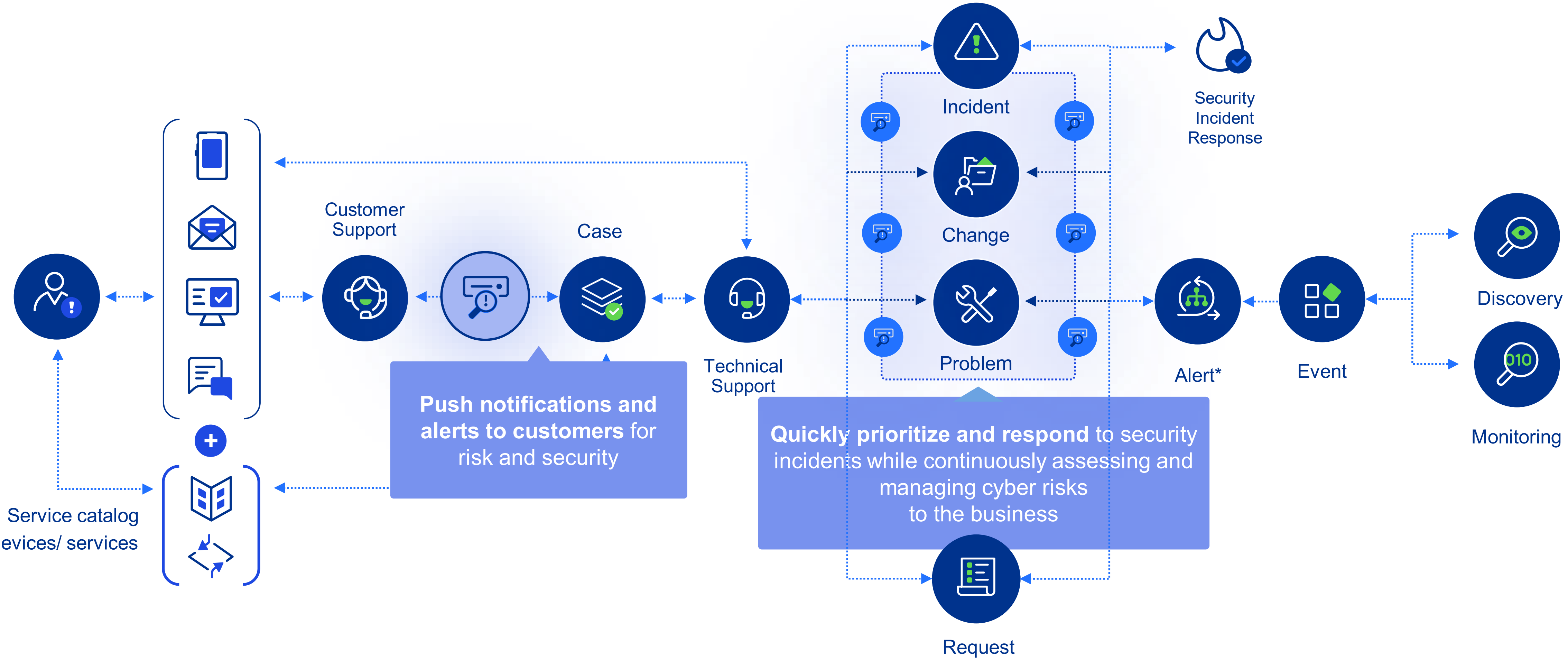
Internal audits

Lack of secure services, at a high cost

With ServiceNow, Technology Providers can effectively manage technology risk and build cyber resilience


servicenow
All risk managed in one platform
Workflow
External Auditors
Vulnerability Manager
Security Operations
Security Incident Response
Risk & Security
Tech and Security Control function
Risk and Compliance teams
Internal audits
Secure service workflows, at a lower cost
Near real-time data

Delivering a more resilient proactive service experience while your business safely executes



Push notifications and alerts to customers for risk and security

Quickly prioritize and respond to security incidents while continuously assessing and managing cyber risks to the business

ServiceNow SecOps summary

01

Security Incident Response

Manage threat exposure proactively by knowing your security posture and quickly prioritize high-impact threats in real time. Ensure cyber Resilience and increase efficiency.

- Risk based prioritization
- Exception management
- Automated response
- Orchestrated playbooks

02

Vulnerability Response

Continuously prioritize vulnerabilities using asset, severity, exploit, and threat intelligence. Reduce your attack surface and respond to critical vulnerabilities faster.

- Assignment and lifecycle tracking
- Exception management
- Automated remediation
- Risk based prioritization

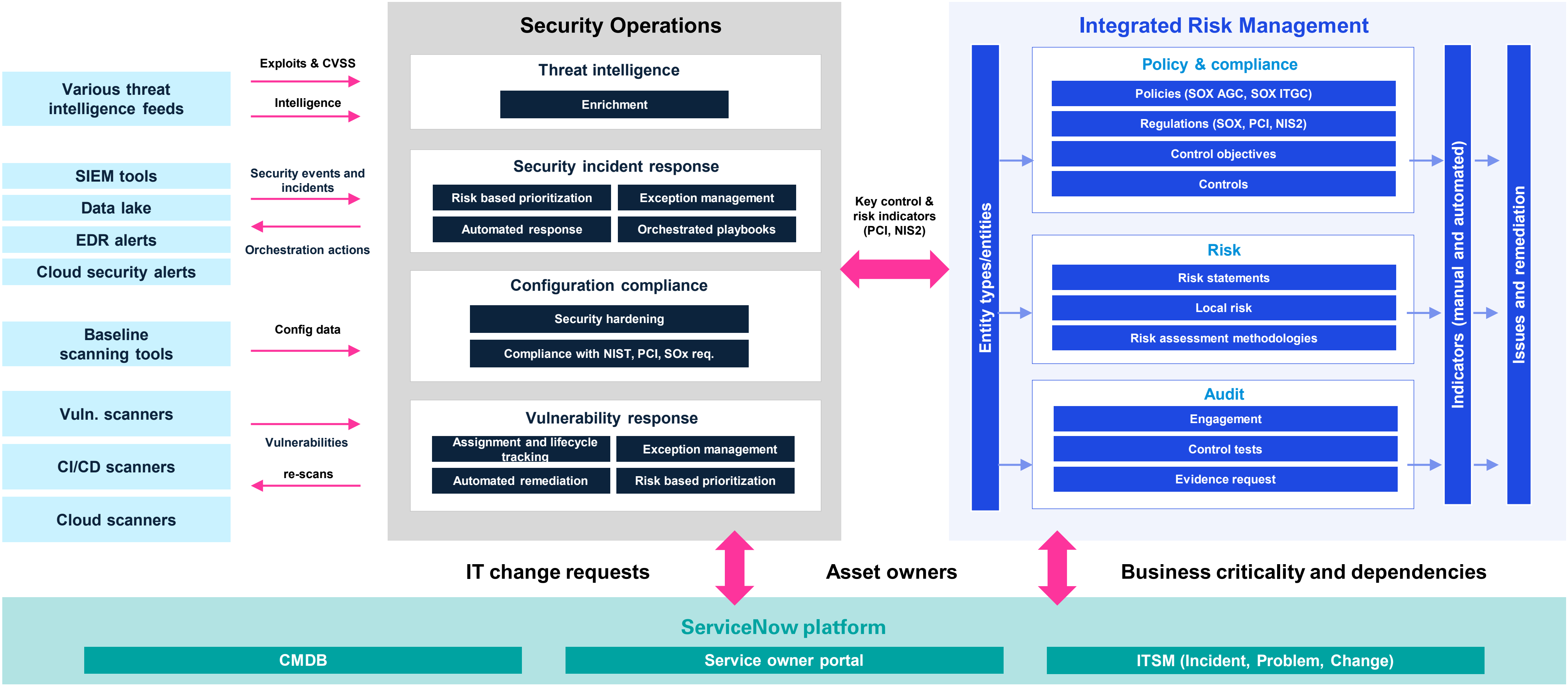
03

Configuration Compliance

Configuration Compliance enables you to identify, prioritize, and remediate vulnerability misconfigured software.

- Security hardening
- Compliance with NIST, PCI, SOx req.

SecOps enables compliance reporting in IRM



Various threat intelligence feeds

Exploits & CVSS

Intelligence

SIEM tools

Data lake

EDR alerts

Cloud security alerts

Security events and incidents

Orchestration actions

Baseline scanning tools

Config data

Vuln. scanners

CI/CD scanners

Cloud scanners

Vulnerabilities

re-scans

Security Operations

Threat intelligence

- Enrichment

Security incident response

- Risk based prioritization
- Exception management
- Automated response
- Orchestrated playbooks

Configuration compliance

- Security hardening
- Compliance with NIST, PCI, SOx req.

Vulnerability response

- Assignment and lifecycle tracking
- Exception management
- Automated remediation
- Risk based prioritization

Key control & risk indicators (PCI, NIS2)

Integrated Risk Management

Entity types/entities

Policy & compliance

- Policies (SOX AGC, SOX ITGC)
- Regulations (SOX, PCI, NIS2)
- Control objectives
- Controls

Risk

- Risk statements
- Local risk
- Risk assessment methodologies

Audit

- Engagement
- Control tests
- Evidence request

Indicators (manual and automated)

Issues and remediation

IT change requests

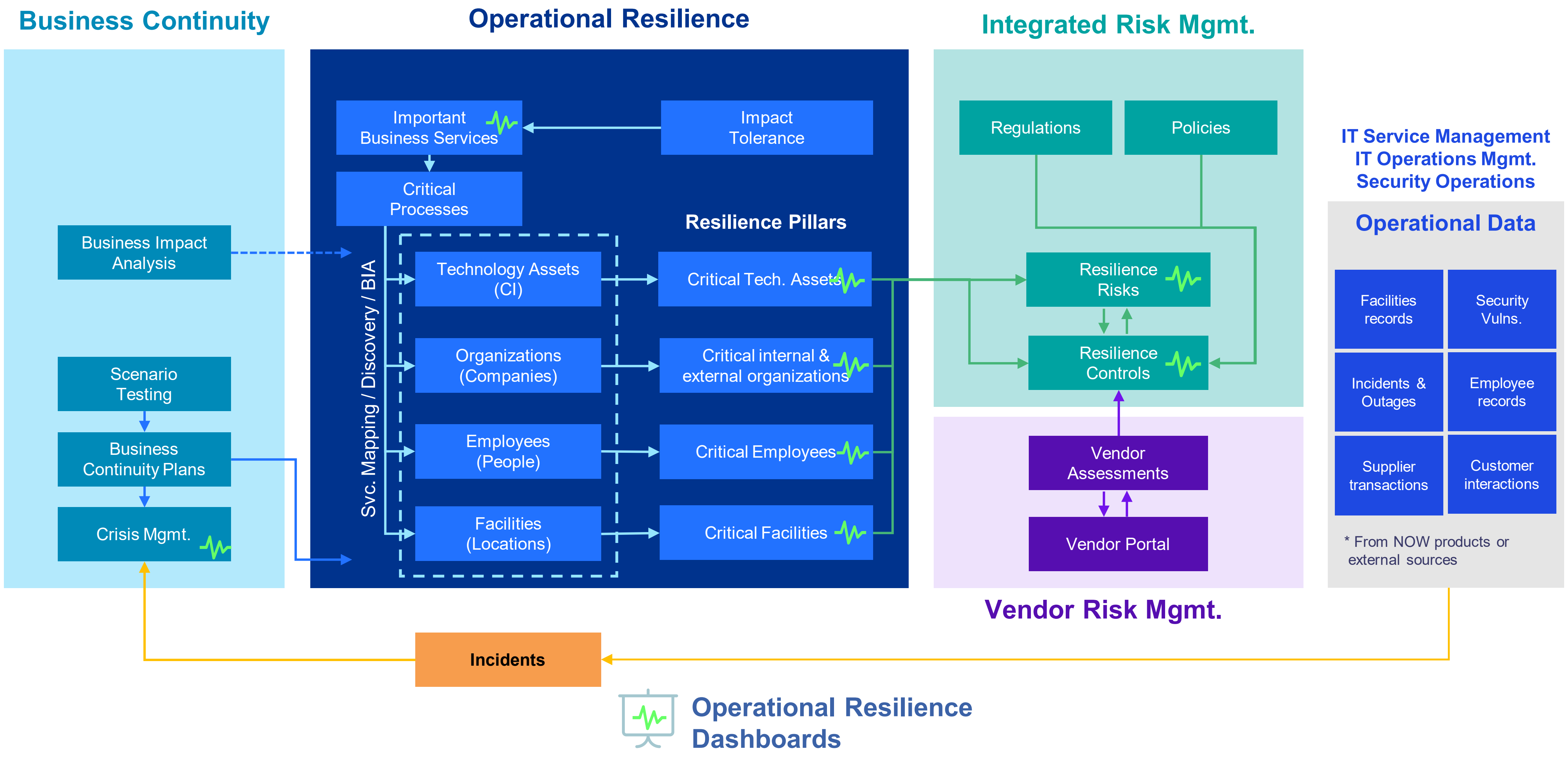
Asset owners

Business criticality and dependencies

ServiceNow platform

- CMDB
- Service owner portal
- ITSM (Incident, Problem, Change)

The operational resilience workflow in ServiceNow



04

Next steps

Next steps to get started

01. **Dedicated project** – establish a workstream in your DORA programme to ensure the incident management and reporting process works end-to-end

02. **Identify** – keys stakeholders, as well as processes and technology needed. Develop a target operating model with clear roles and responsibilities.

03. **Analyse** – identify missing data, people, process and technology needed, along with a remdiation plan for your target state

04. **Deliver** – execute the transformation activity and rollout to teams. Effective transformation needs to include all elements, in particular with focus on people

05. **Test and validate** – run repeated scenarios to validate the people, process, and technology are able to operate in real-time

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