Understanding DORA: Your Path to Achieving Resiliency

Demystifying the Digital Operational Resilience Act (DORA) to help you power resilience and meet obligations

Agenda

- Introductions
- DORA overview
- Impact of DORA Regulations
- Strategies and Key Takeaways
- Real-Life Examples of Regulations in Action
- Walkthrough-What Do DORA Regulations Look Like in Practice?
- Questions

FUSION
RISK MANAGEMENT

Introductions

Rich Cooper

Global Head of Financial Service Go-To-Market

Fusion Risk Management

Rui Dos Ramos

Senior Solutions Engineer

Fusion Risk Management

Shawn Lonergan

Partner, Technology & Operational Resilience

PwC

Fiona Marschollek

Senior Consultant, DORA SME

PwC

Mandy Leavell

Senior Product Marketing Manager

Fusion Risk Management

DORA Overview

What is DORA and who does it impact?

FUSION RISK MANAGEMENT

Poll 1

How familiar are you with DORA regulations?

‘Digital Operational Resilience’ – what does it really mean?

“

The ability of a finance entity to **build**, **assure** and **review** its operational integrity and reliability by ensuring…

… either directly or indirectly through the use of services provided by **ICT third-party services providers**,…

… the **full range of ICT-related capabilities** needed to address the security of the network and information systems which a financial entity uses…

… and which support the **continued provision** of financial services and their quality, including **throughout disruption**”

”

DORA creates a binding framework for the management of ICT and cyber risks for financial entities in the EU and globally

Purpose

DORA (**D**igital **O**perational **R**esilience **A**ct) defines detailed and comprehensive regulations for digital operational resilience at EU level

Harmonize local regulations in the financial sector across the EU Member States, thereby:

- ensuring that financial entities and third-party providers (TPP), respond to and timely recover from all types of ICT-related disruptions
- empowering financial supervisory authorities to monitor and audit financial entities and their third-party ICT providers more closely
- introducing a uniform incident reporting mechanism incl. knowledge sharing

Key control areas

Governance

Strengthen active role of management board

ICT Risk Management

Tactical, organisational and technical cybersecurity capabilities

Incident Reporting

Detection, reporting and management of ICT-related incidents

Resilience Testing

Regular testing of resilience measures and critical systems

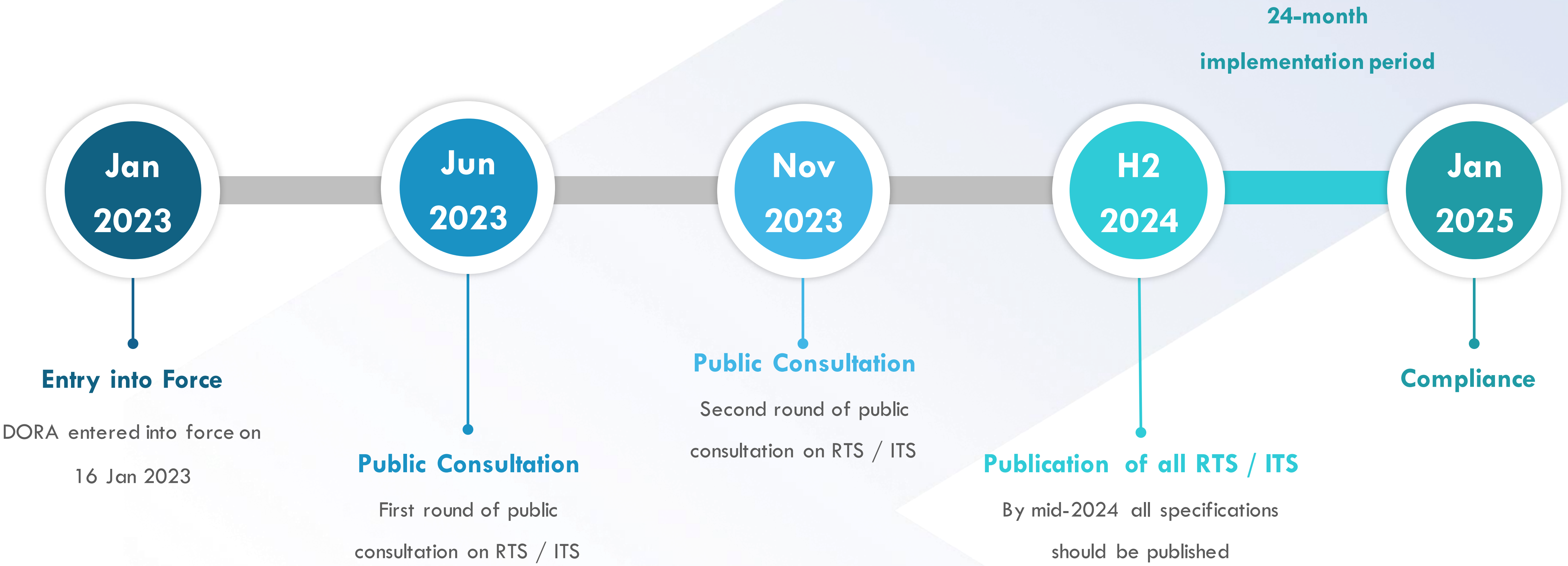
3rd party risk Mgmt.

Advanced monitoring and management of 3rd party risk

Information Sharing

Exchange threat intelligence, best practice, etc. among trusted communities

The 24-month implementation period of DORA is already underway



24-month implementation period

Jan 2023

Jun 2023

Nov 2023

H2 2024

Jan 2025

Entry into Force

DORA entered into force on 16 Jan 2023

Public Consultation

First round of public consultation on RTS / ITS

Public Consultation

Second round of public consultation on RTS / ITS

Publication of all RTS / ITS

By mid-2024 all specifications should be published

Compliance

DORA requires an end-to-end approach towards ICT risk management and operational resilience

Operational Resilience, is the ability of an organization to deal with risks of disruption to processes and applications that support its business while maintaining its viability.

The Digital Operational Resilience Framework ultimately aims **at identifying, assessing, mitigating and managing risks** that may impact critical functions related to the organization's core business.

Key action areas

- Identify and map critical functions
- Collect data and information
- Define impact tolerances
- Perform (stress) scenario testing
- Monitor and mitigate risks

Strategic takeaways and key benefits of implementing DORA beyond compliance

Consider DORA as a Strategic Opportunity to deliver long-term value!

- **"Don't reinvent the wheel"** - Improve already existing information in both governance and management models and avoid the "from scratch" approach
- **Improve Local Best Practices** – Use of possible Group-wide best practices or best practices developed within individual business units

Adopt a cross-functional approach - DORA is not simply an ICT and/or Cyber topic!

- **Synergies** – To achieve the objectives of Digital Operational Resilience, strong collaboration across all impacted stakeholders is essential to ensure initiatives are not undertaken in a 'silo approach'.
- **Stakeholder Committment** – Considering the transversal impact of the Regulation, the involvement and commitment of a significant number of players from different functions is necessary.

Make best use of the time available!

- **Digital Operational Resilience Strategy** – Focus on driving activities and initiatives with no dependencies on RTSs, then shifting focus on implementing the core aspects of digital operations resilience.
- **Cost / Investment Planning** - Spreading initiatives over the 2 year period will allow for proper financial management, also considering the capacity needs for the "run" management after implementation phase.

Beyond the Pillars of DORA

Practical applications of DORA regulation to set your business on the best track to resilience

FUSION
RISK MANAGEMENT

Poll Two

What is the biggest obstacle to implementing DORA in alignment with Operational Resilience?

FUSION RISK MANAGEMENT

Incident: Third-Party Risk

Your Third-Party Team receives an alert that the individual credit agency you use for credit checks on auto loans has had its IT security score drop.

A Proactive Approach

The Third-Party Risk team looks at your vendor to see dependencies. However, they want to go beyond simply understanding dependencies and decide to perform scenario analyses.

You run some scenarios against the impact tolerances of your important business services to see if there are any potential breaches of tolerance.

After running testing on various scenarios, you note the potential downtime from the vendor service being unavailable exceeds the risk tolerance.

The team brings this concern to the Executive Team. The data from your scenarios allow you to go to leadership with substance, confidence, and facts they can act on.

The Executive team evaluates their options: As there are three major providers, leadership decides they can accept the risk of losing one of the three agencies.

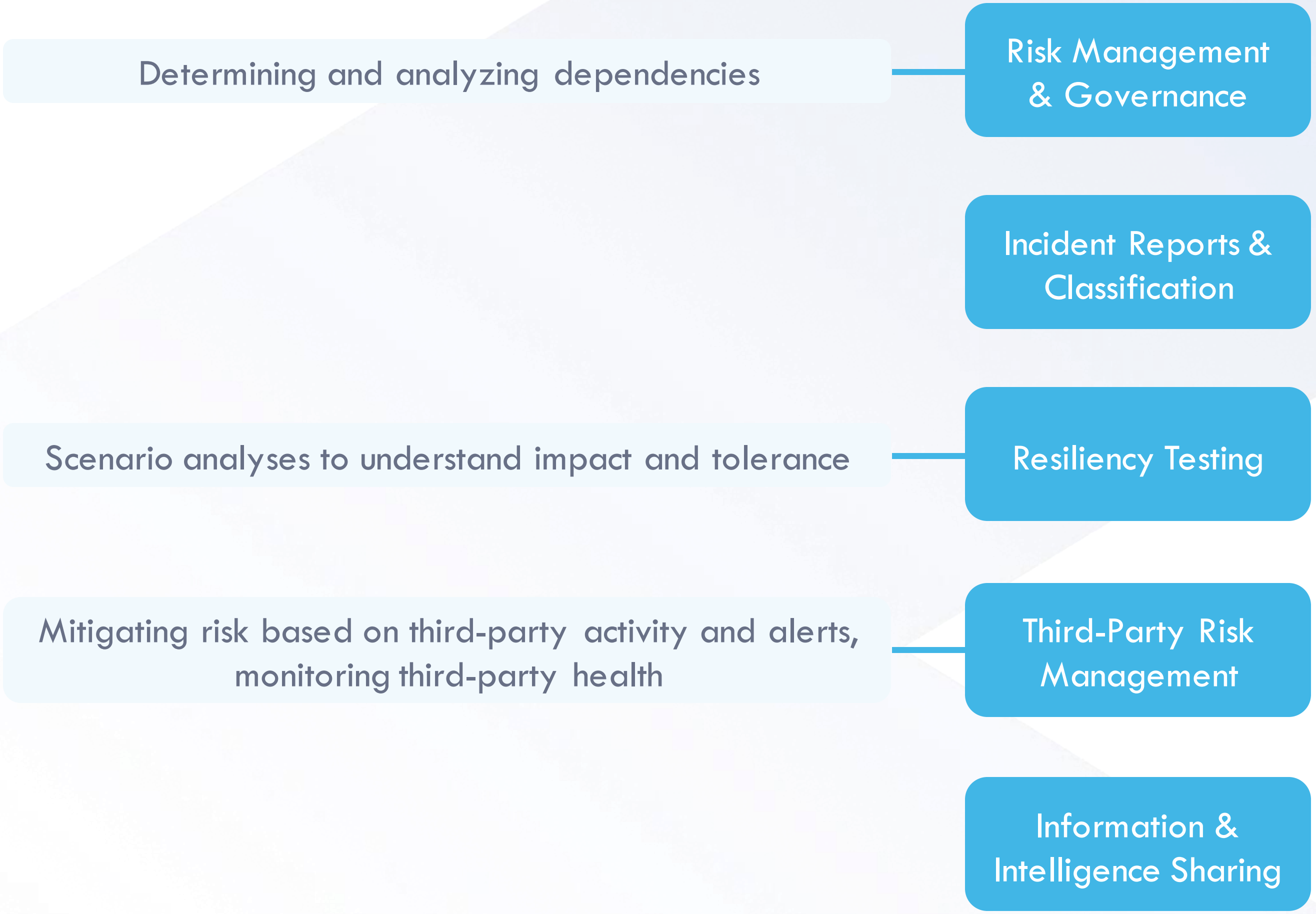
They document the acceptance and the control; Should one agency become unavailable, you will still be able to fulfill your customer obligations via the other two.

DORA Pillars Involved:

1. Risk Management and Governance
2. Incident Reports and Classification
3. Resiliency Testing
4. Third-Party Risk
5. Oversight Framework- Information and Intelligence Sharing

Review

Third-Party Event



Determining and analyzing dependencies — Risk Management & Governance

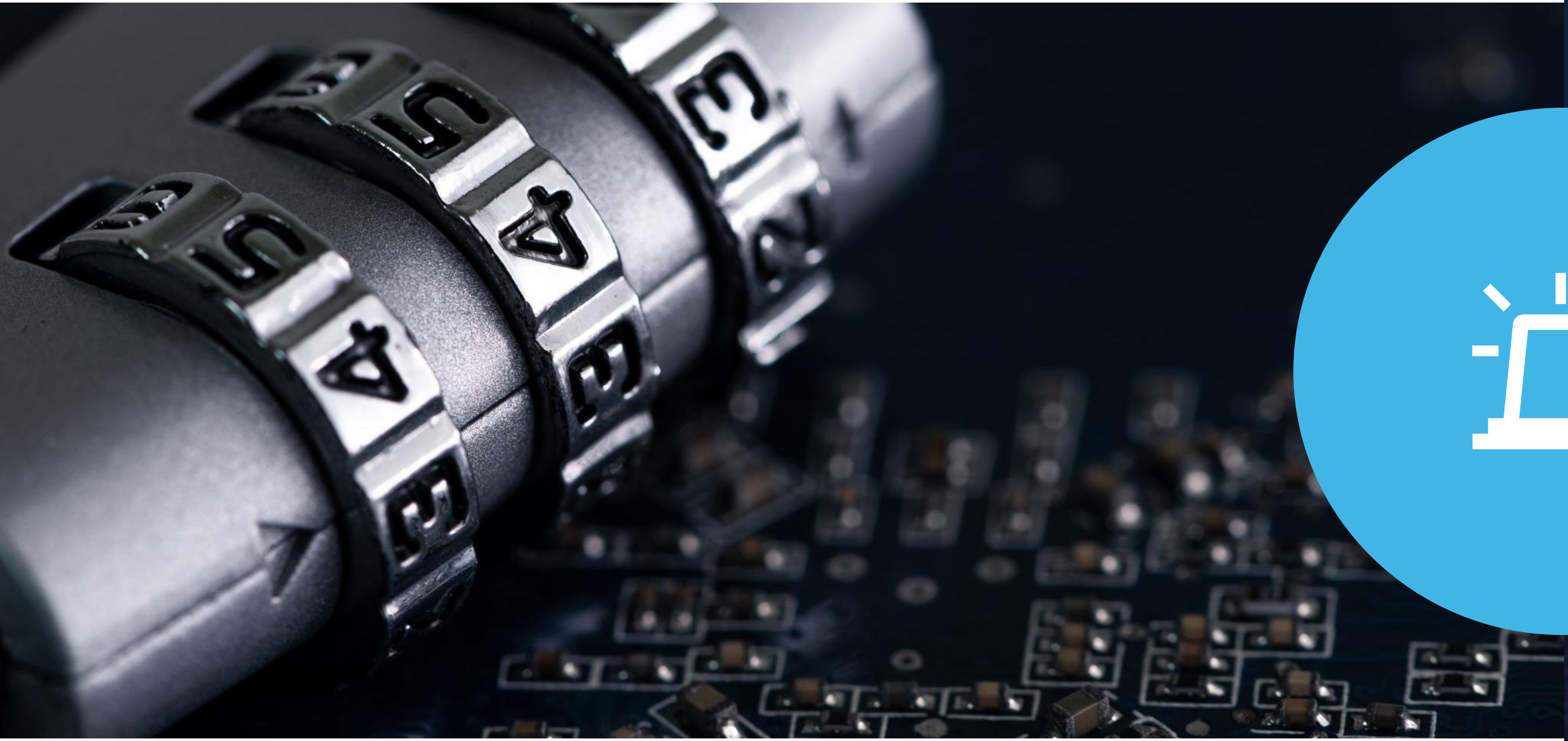
Incident Reports & Classification

Scenario analyses to understand impact and tolerance — Resiliency Testing

Mitigating risk based on third-party activity and alerts, monitoring third-party health — Third-Party Risk Management

Information & Intelligence Sharing

Incident: Ransomware Attack



Your bank becomes a victim of a ransomware attack. One of your important data sets is encrypted on an application.

All Hands on Deck for Recovery

The IT Team investigates the threat and identifies that it is a real ransomware attack. They initiate their response plan.

They determine where the data set is located, and analyze which operations and services are dependent on this data. This information is shared with the Crisis Management Team (CMT).

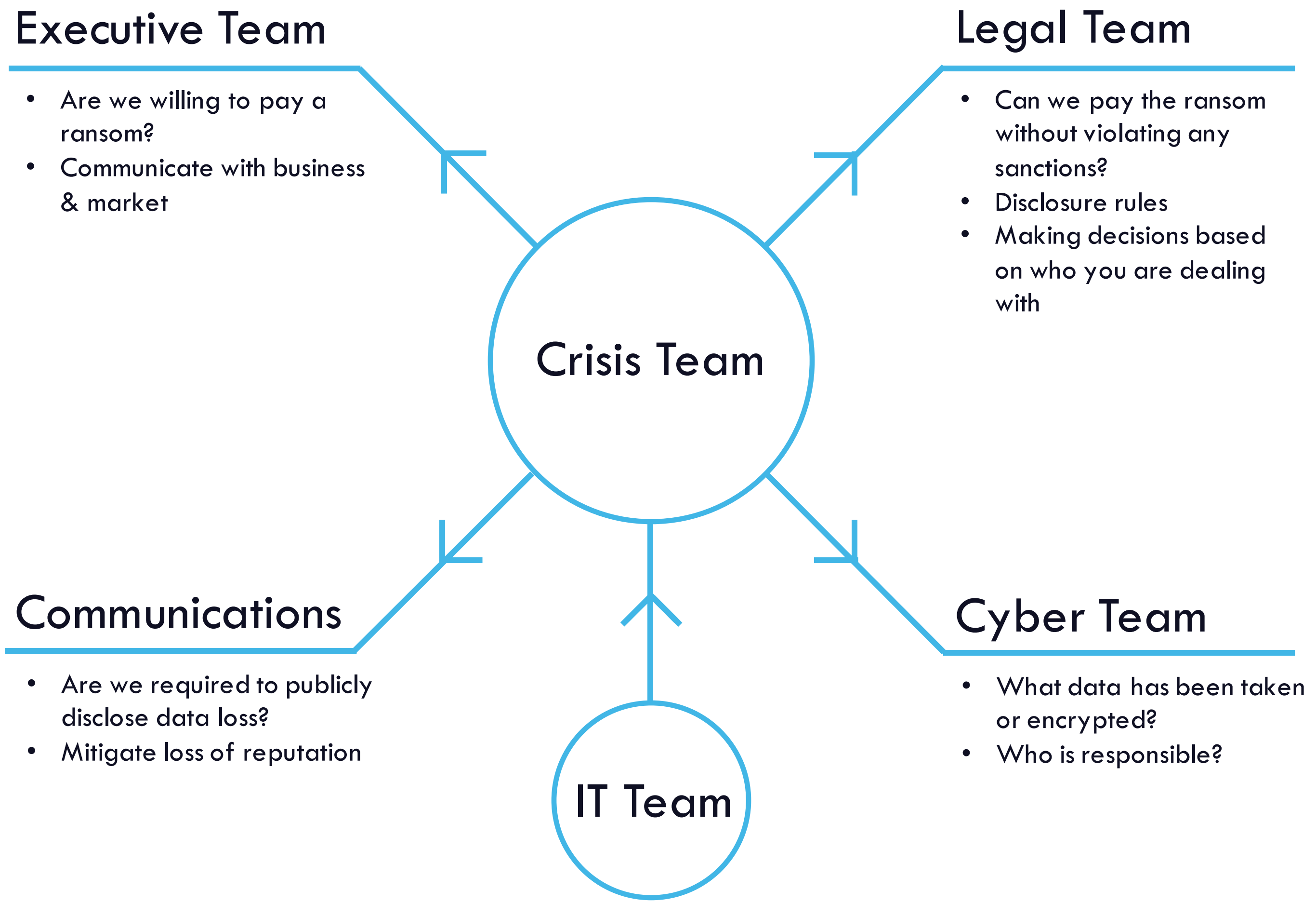
The CMT validates that the business' credit line is dependent on the affected data set. This impacts Settlement Transactions, one of the most important services to your business.

The CMT then opens a new issue and starts to activate the necessary teams to manage a ransomware attack.

DORA Pillars Involved:

1. Risk Management and Governance
2. Incident Reports and Classification
3. Resiliency Testing
4. Third-Party Risk
5. Oversight Framework- Information and Intelligence Sharing

All Hands on Deck for Recovery



Executive Team

- Are we willing to pay a ransom?
- Communicate with business & market

Legal Team

- Can we pay the ransom without violating any sanctions?
- Disclosure rules
- Making decisions based on who you are dealing with

Crisis Team

Communications

- Are we required to publicly disclose data loss?
- Mitigate loss of reputation

IT Team

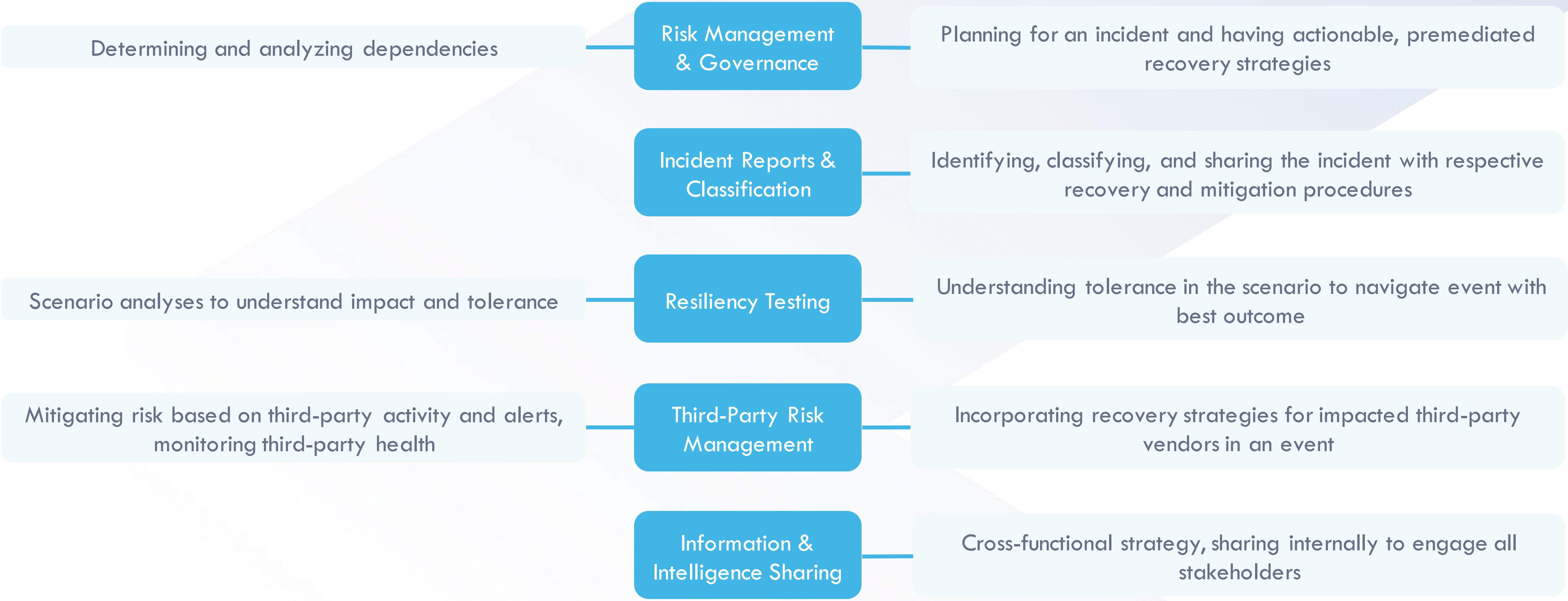
Cyber Team

- What data has been taken or encrypted?
- Who is responsible?

DORA Pillars Involved:

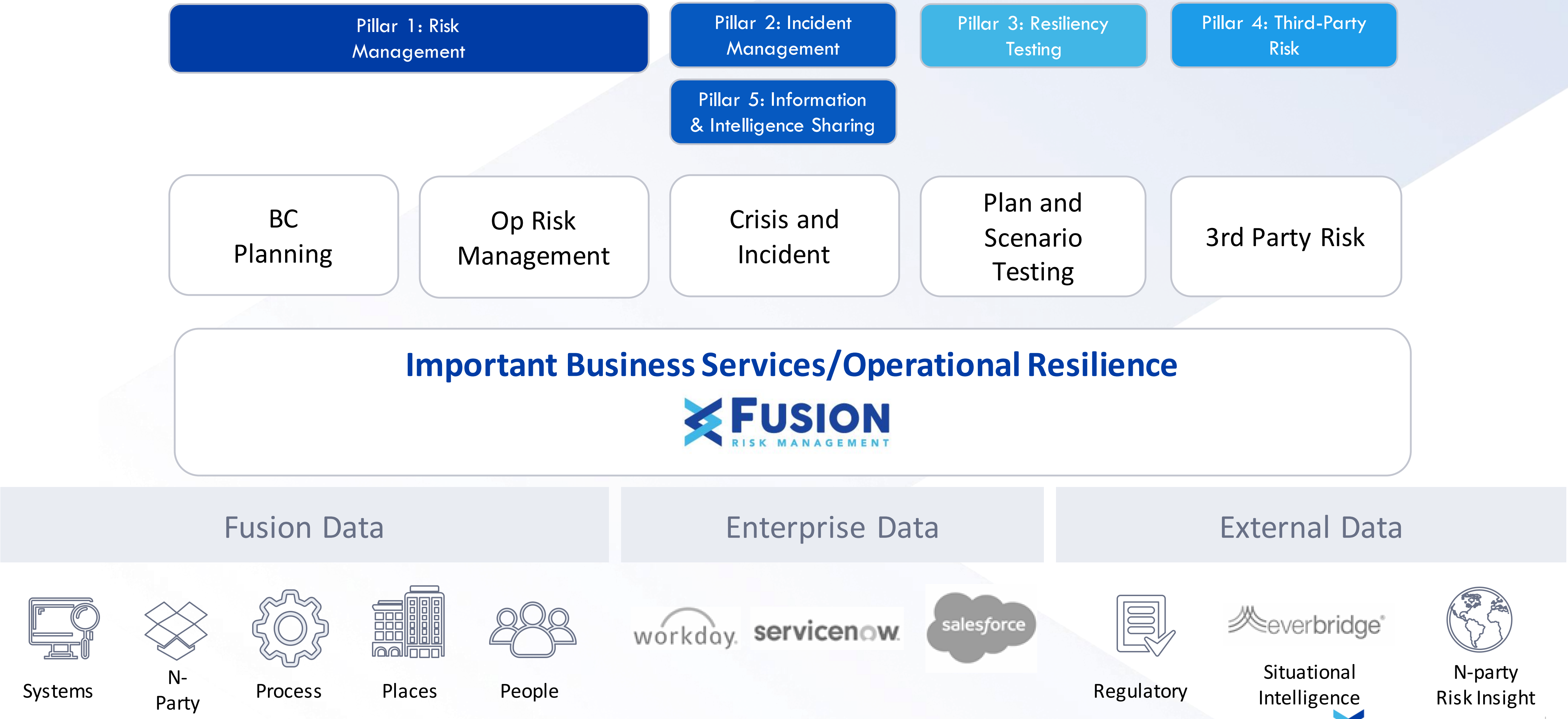
1. Risk Management and Governance
2. Incident Reports and Classification
3. Resiliency Testing
4. Third-Party Risk
5. Oversight Framework- Information and Intelligence Sharing

Review



Third-Party Event		Ransomware Attack
Determining and analyzing dependencies	Risk Management & Governance	Planning for an incident and having actionable, premediated recovery strategies
	Incident Reports & Classification	Identifying, classifying, and sharing the incident with respective recovery and mitigation procedures
Scenario analyses to understand impact and tolerance	Resiliency Testing	Understanding tolerance in the scenario to navigate event with best outcome
Mitigating risk based on third-party activity and alerts, monitoring third-party health	Third-Party Risk Management	Incorporating recovery strategies for impacted third-party vendors in an event
	Information & Intelligence Sharing	Cross-functional strategy, sharing internally to engage all stakeholders

Fusion is the hub that unifies your DORA compliance efforts



Pillar 1: Risk Management

Pillar 2: Incident Management

Pillar 3: Resiliency Testing

Pillar 4: Third-Party Risk

Pillar 5: Information & Intelligence Sharing

BC Planning

Op Risk Management

Crisis and Incident

Plan and Scenario Testing

3rd Party Risk

Important Business Services/Operational Resilience

FUSION RISK MANAGEMENT

Fusion Data

Enterprise Data

External Data

Systems

N-Party

Process

Places

People

workday. servicenow salesforce

Regulatory

everbridge

Situational Intelligence

N-party Risk Insight

Questions

FUSION
RISK MANAGEMENT

Rich Cooper

Global Head of Financial Service Go-To-Market

Fusion Risk Management

Linkedin.com/in/richard-cooper/a2782b

Rui Dos Ramos

Senior Solutions Engineer

Fusion Risk Management

Linkedin.com/in/ruidosramos

Shawn Lonergan

Partner, Technology & Operational Resilience

PwC

Linkedin.com/in/shawn-lonergan

Fiona Marschollek

Senior Consultant, DORA SME

PwC

Linknedin.com/in/fiona-marschollek

FUSION RISK MANAGEMENT

Thank You

fusionrm.com

in @fusion-risk-management

f @FusionRiskManagement

@FusionRiskMgmt