Navigating DORA: Identifying Important Business Functions and Mastering Incident Management

FUSION
RISK MANAGEMENT

pwc

Agenda

- Introductions
- Identifying Critical Business Functions
- Incident Management
- Practical Application
- Questions

Introductions

Rich Cooper

Global Head of Financial Service Go-To-Market

Fusion Risk Management

Ryan Shea

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

Poll

Do you consider your DORA initiative to be integrated into your operational resilience program?

Results:

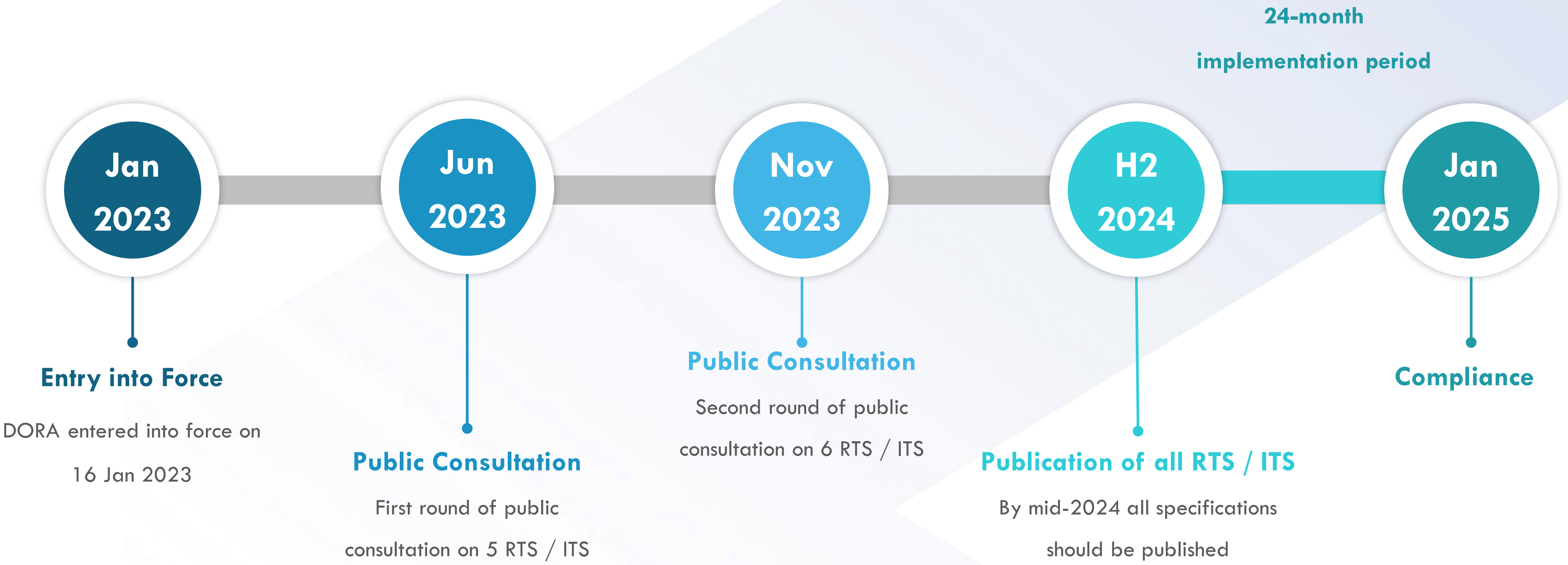
Yes, fully integrated | 5%
Yes, but still working on integration | 35%
No, it’s a standalone project | 14%
No, we don’t have a DORA initiative yet | 46%

FUSION RISK MANAGEMENT

Identifying Important Business Functions

FUSION RISK MANAGEMENT

The 24-month implementation period of DORA is already underway



24-month implementation period

Jan 2023

Entry into Force

DORA entered into force on 16 Jan 2023

Jun 2023

Public Consultation

First round of public consultation on 5 RTS / ITS

Nov 2023

Public Consultation

Second round of public consultation on 6 RTS / ITS

H2 2024

Publication of all RTS / ITS

By mid-2024 all specifications should be published

Jan 2025

Compliance

What is a critical or important function?

With material impact on

- the financial performance of a financial entity
- The soundness or continuity of its services and activities
- Compliance and the real economy and financial stability

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.

Defining critical or important functions within DORA

Financial performance

- Financial impact analysis
- Risk quantification
- …

Robustness or continuity of services

- Protection goals (CIA rating)
- Business Impact Analysis
- Impact Tolerances

Compliance

- Depending on applicable national/intl. regulation

Market impact

- Client base
- Substitutability
- Time criticality
- …

Why DORA requires you to identify your critical or important functions

- Cyber and ICT risks are inevitable
- Minimize the impact of critical incidents on your core business
- Identify your dependencies to 3rd parties
- Test your capabilities and measures to ensure the continuity of your critical or important functions

Key action areas

IDENTIFY
Entire information domain & dependencies to 3rd parties

PROTECT & PREVENT
ICT security policies, procedures, protocols to ensure resilience of ICT systems

DETECT
Threats and anomalous activities incl. regular testing of all critical ICT systems

RESPOND
BCM and ITSCM policies and measures to ensure continuity of critical functions

RECOVER
Backup and restore, incl. redundant capabilities identical to primary site

Realignment toward a ‘Business function’ led view is vital

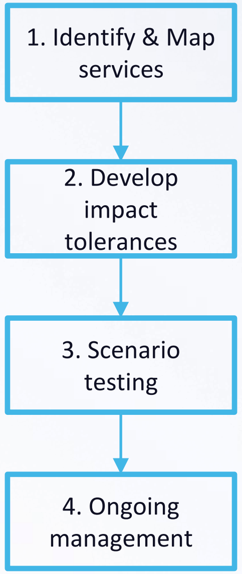
Existing core capabilities are typically siloed

Firms often have established resilience capabilities in their business, but these may be siloed and not coherently mapped to critical or important functions.

- Cyber security
- Capacity management
- Service operations
- Incident management
- Capability & resources
- Sourcing & external dependencies
- Change management
- Human resources management
- Continuity management
- Physical security

Realign

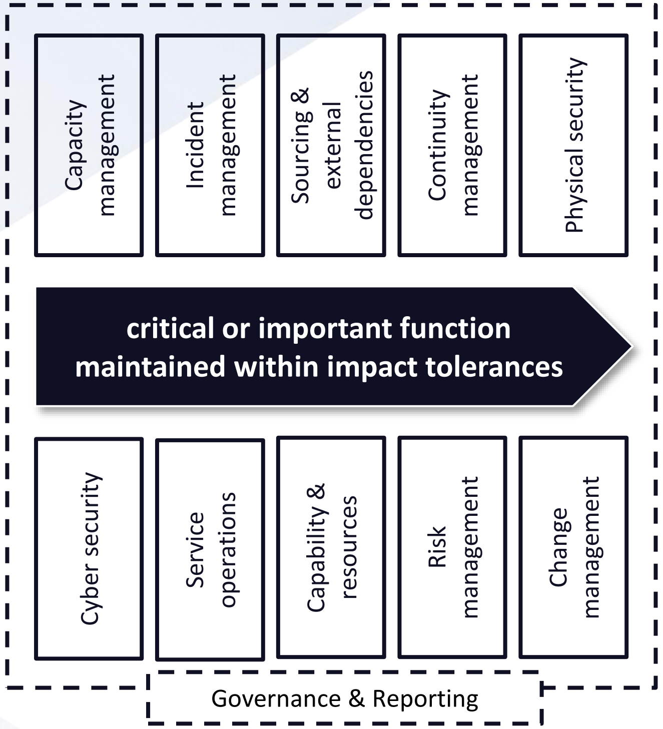
Firms need to undertake a process to identify their critical or important functions and understand the key capabilities that support their delivery



1. Identify & Map services
2. Develop impact tolerances
3. Scenario testing
4. Ongoing management

Align existing activities around business services

Firms must then align existing resilience capabilities to support the provision of each critical or important function and maintain these within the agreed impact tolerances. They must also perform gap assessment of their resilience capabilities to ensure they are fit for purpose.



Incident Management

Poll

Do you have a process in place to review all ICT-related incidents for reporting requirements?

Results:

Yes, internally to our management board | 42%
Yes, to regulators | 5%
Yes, to management board AND regulators | 35%
No, not currently | 18%

Incident Management Process

- End-2-end management process
- Harmonized reporting of major ICT-related incidents
- Common classification methodology (*RTS Update*)
- Centralized reporting at EU level

Incident management is a fundamental and necessary process to avoid or **minimize the economic and reputational impact** of an incident and thus be able to restore normal service operations quickly

DORA introduces specific mechanisms for handling ICT-related incidents

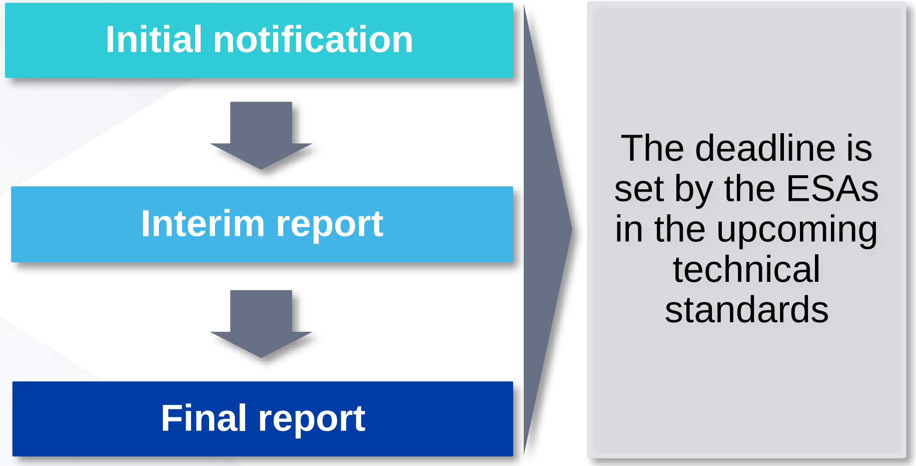
Objective

ICT-related incident management process to detect, manage, and report ICT-related incidents.
Record all ICT-related incidents and significant cyber threats.

Strategic Considerations

- Introduce and implement an ICT-related **incident management process** to identify, track, log, categorize and classify ICT-related incidents
- ICT-related incidents should be **properly classified** and their impact must be assessed
- Major ICT-related incidents should be **reported** to management and the relevant authority
- **Notifying clients** exposed to significant cyber threats and informing them of protective measures

Key Requirements



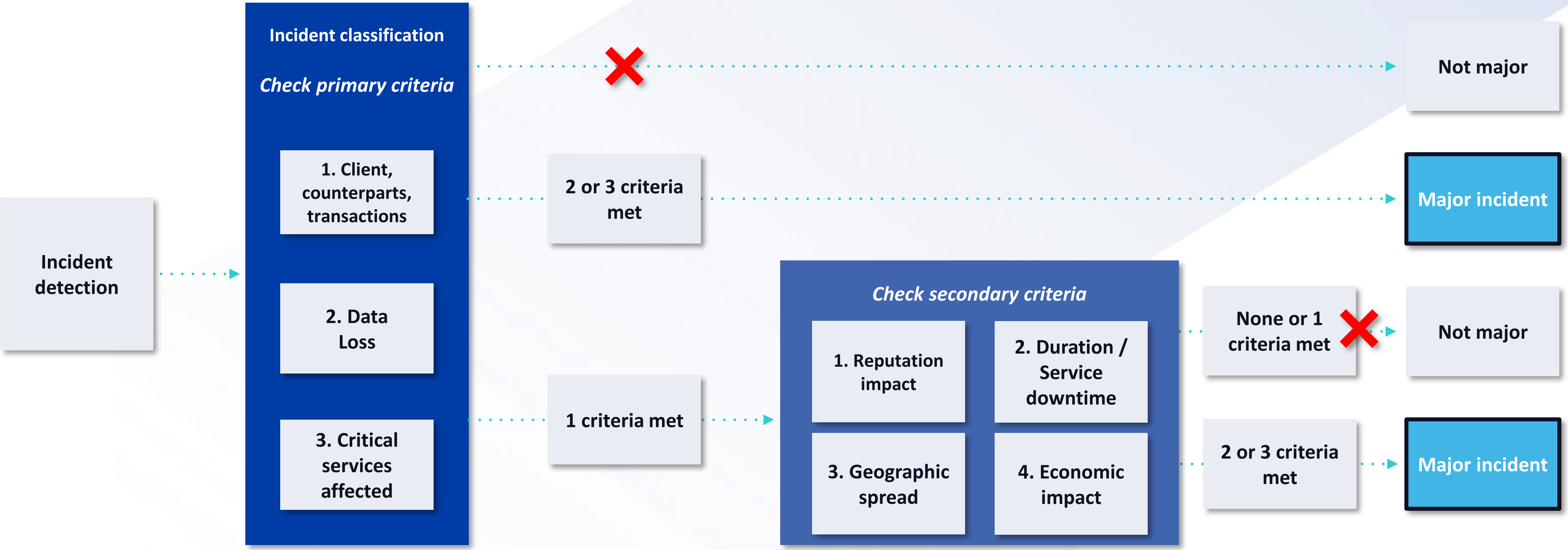
Initial notification

Interim report

Final report

The deadline is set by the ESAs in the upcoming technical standards

Classification of major incidents according to the RTS



Incident detection

Incident classification

Check primary criteria

1. Client, counterparts, transactions

2. Data Loss

3. Critical services affected

Not major

2 or 3 criteria met

Major incident

1 criteria met

Check secondary criteria

1. Reputation impact

2. Duration / Service downtime

3. Geographic spread

4. Economic impact

None or 1 criteria met

Not major

2 or 3 criteria met

Major incident

Important Business Functions and Incident Management in Practice

Looking through a real-life example of a ransomware attack

FUSION
RISK MANAGEMENT

Recap: Understanding DORA: Your Path to Achieving Resiliency

Your organization needs to take a cross-functional approach to implementing DORA regulation

DORA is a strategic opportunity to deliver long-term value and implement Op Res best practices

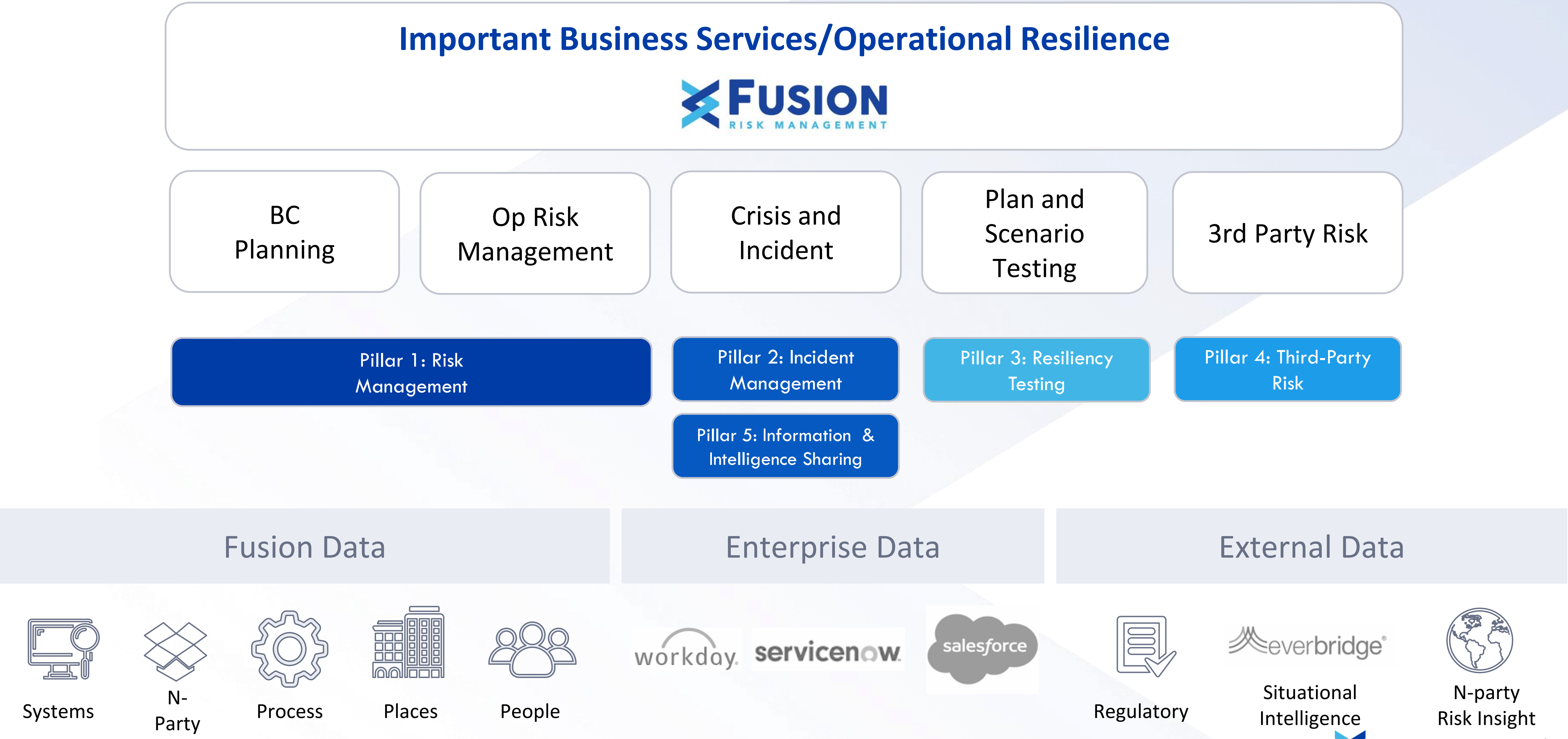
DORA is NOT just an IT problem; it's a business problem

With the 24-month implementation window underway, it is important to get started as soon as possible

The organizations who implement DORA most successfully tend to begin with identifying their important business functions

Focus on breaking down informational and team silos, and bringing your data together in one place

Fusion is the hub that unifies your DORA compliance efforts



Important Business Services/Operational Resilience

FUSION RISK MANAGEMENT

BC Planning

Op Risk Management

Crisis and Incident

Plan and Scenario Testing

3rd Party Risk

Pillar 1: Risk Management

Pillar 2: Incident Management

Pillar 5: Information & Intelligence Sharing

Pillar 3: Resiliency Testing

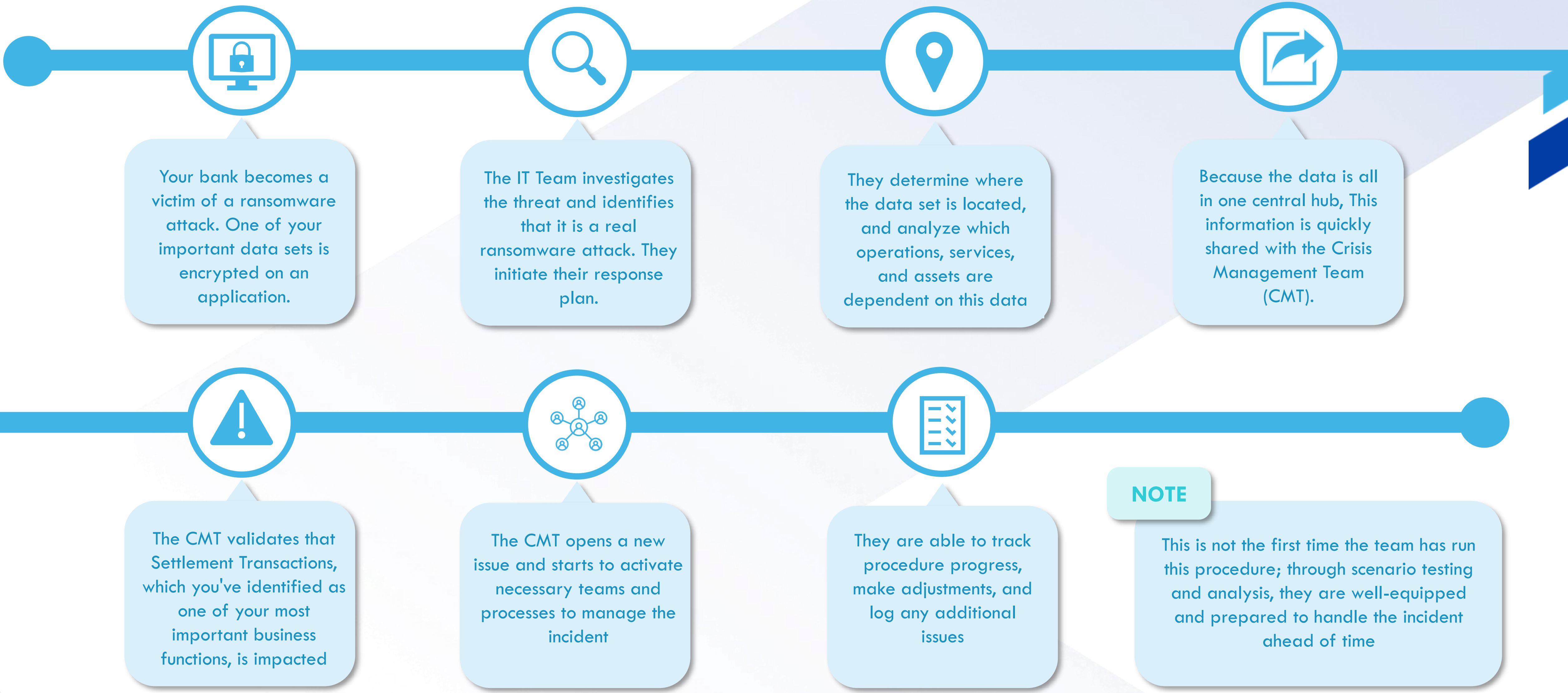
Pillar 4: Third-Party Risk

Fusion Data

Enterprise Data

External Data

Response: Ransomware Attack



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

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, services, and assets are dependent on this data

Because the data is all in one central hub, This information is quickly shared with the Crisis Management Team (CMT).

The CMT validates that Settlement Transactions, which you've identified as one of your most important business functions, is impacted

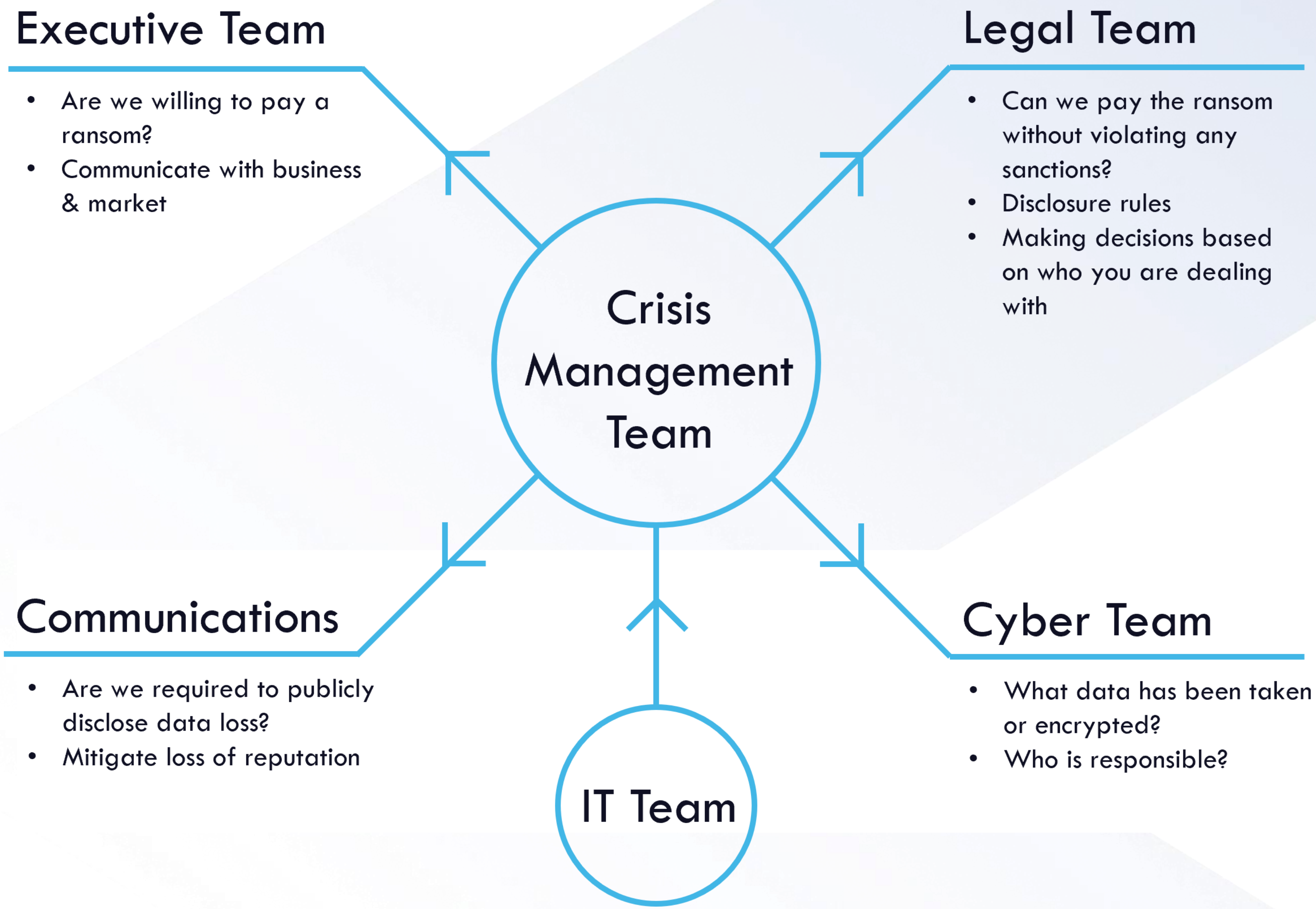
The CMT opens a new issue and starts to activate necessary teams and processes to manage the incident

They are able to track procedure progress, make adjustments, and log any additional issues

NOTE

This is not the first time the team has run this procedure; through scenario testing and analysis, they are well-equipped and prepared to handle the incident ahead of time

All Hands on Deck



Crisis Management Team

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

Communications

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

Cyber Team

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

IT Team

Questions?

Thank You!

Rich Cooper

Global Head of Financial Service Go-To-Market

Fusion Risk Management

Linkedin.com/in/richard-cooper/a2782b

Shawn Lonergan

Partner, Technology & Operational Resilience

PwC

Linkedin.com/in/shawn-lonergan

Ryan Shea

Senior Solutions Engineer

Fusion Risk Management

Linkedin.com/in/ryan-shea-45383b98/

Fiona Marschollek

Senior Consultant, DORA SME

PwC

Linknedin.com/in/fiona-marschollek

FUSION RISK MANAGEMENT