Bolstering Third-Party Risk Management Under DORA Regulation

FUSION RISK MANAGEMENT

pwc

Agenda

- Introductions
- Scope of DORA
- Understanding Third-Party Risk Management Under DORA
- Managing Risk Across a Third-Party Lifecycle
- Practical Application
- Questions

FUSION
RISK MANAGEMENT

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

Are your third-party risk management leaders involved in your DORA program?

FUSION RISK MANAGEMENT

pwc

Ensuring Resilience with Your Third Party Vendors

FUSION RISK MANAGEMENT

pwc

ICT Third-Party Risk Management

- What is the scope of DORA?
- Understanding Third party risk management in the context of DORA
- Discussing the impact of third parties on your important business functions

DORA affects financial entities within the EU but by extension also global institutions and 3rd party providers

Scope

All participants on the financial markets, including banks, insurance undertakings and intermediaries, asset managers, crypto asset providers and more - below is a non-exhaustive list

Credit Institutions	Crypto-asset service providers	Occupational retirement provision
Payment Institutions	Trading venues	Credit rating agencies
Electronic money institutions	(Re)Insurance undertakings	Crowdfunding service providers
Investment firms	(Re)Insurance intermediaries	Account information service providers

ICT third-party service providers

Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards

Proportionality Principle

Size and overall risk profile, as well as the nature, scope and complexity of their services, activities and operations

Understanding Third party risk management in the context of DORA

What is new in DORA?

Principles for monitoring risks arising from ICT service providers, both in terms of ICT procurement and outsourcing arrangements

Harmonization of essential elements for contractual relationships with ICT 3rd parties at all stages of the third party management life-cycle.

Convergence of Supervisory approaches at European level by establishing a unique Oversight framework

3rd party risk Mgmt.

Advanced monitoring and management of 3rd party risk

New terminology

No differentiation between different forms of “outsourcing”

Service-led view

Focus pivots to ICT service-led view instead of service provider-view

Criticality rating

Criticality rating based on business-led view on critical or important functions

The broad definition of ‘ICT service’ requires a risk-based approach

ICT Service

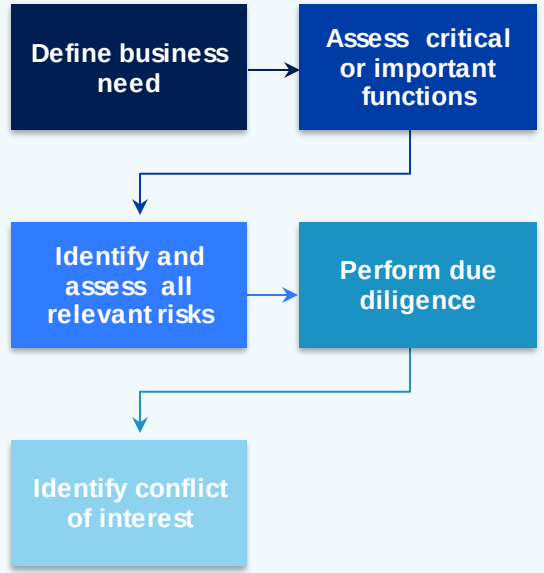
A digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis. This definition includes among others:

- Software licensing
- Data provision & data analysis
- Network material & services
- ICT helpdesk & incident mgmt.
- Hardware rental
- Cloud services & non-cloud data storage
- ICT consulting
- ICT risk mgmt. and audit

ICT services supporting critical or important functions

Policy on the use of ICT services supporting critical or important functions

Ex ante risk assessment	Selection process	Governance & approval processes
Due diligence	Monitoring of risks	Exit strategy & termination



Third-party risk must be managed across the entire 3rd party lifecycle

Pre contract

- **Define business need**
- **Asses the criticality** of the service that is outsourced
- **Identify & assess <u>all</u> risks** associated with the provided service, esp. concentration and sub-outsourcing risks
- **Perform due diligence** on 3rd party ICT provider
- Identify & assess potential conflicts of interest

Contract

- **Implement minimum contractual requirements** for all ICT service providers
- **Extensive audit rights** and ICT testing rights
- **Include informations security requirements**
- **Report annally to the authorities** on all ICT service contracts

Ongoing

- **Assess and ongoing monitoring** of 3rd party risk
- **Define and assess KPIs** and control indicators
- **Monitor SLAs** and performance
- **Maintain the information register** for all ICT suppliers and supply chains

Post contract

- **Develop termination clauses and exit strategies** for certain contingency cases
- **Define criteria for activation** of exit strategies
- **Define & implement operational strategies/ plans** in case of early termination of the contract
- **Put in place effective measures** for recovery of data

Strategic takeaways to implement effective TPRM in DORA

Strategy and Governance

- Integrate ICT Third Party Risk Management Strategy as an integral part into overall ICT Risk Management framework
- The management body bears the ultimate responsibility for managing third party risk & continuously and actively engages in the control and monitoring of contractual arrangements

Cross-functional collaboration

- Establish closer relationships between teams responsible for managing third party service performance and risk
- Enhance handovers between business units, internal controls and other relevant units to facilitate monitoring of third party risks

Group-wide consistency

- Ensure that the policy on the use of ICT services supporting critical or important functions by ICT third party risk providers is applied consistently and coherently across the Group
- Perform the ex ante risk assessment at entity, sub-consolidated and consolidated level, where appropriate

Achieving DORA Compliance with Technology

A real-life example of how DORA regulation can help your third-party risk management strategy

FUSION RISK MANAGEMENT

Recap: Understanding and Navigating DORA

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 3: Resiliency Testing

Pillar 4: Third-Party Risk

Pillar 5: Information & Intelligence Sharing

Fusion Data

Systems

N-Party

Process

Places

People

Enterprise Data

workday. servicenow salesforce

External Data

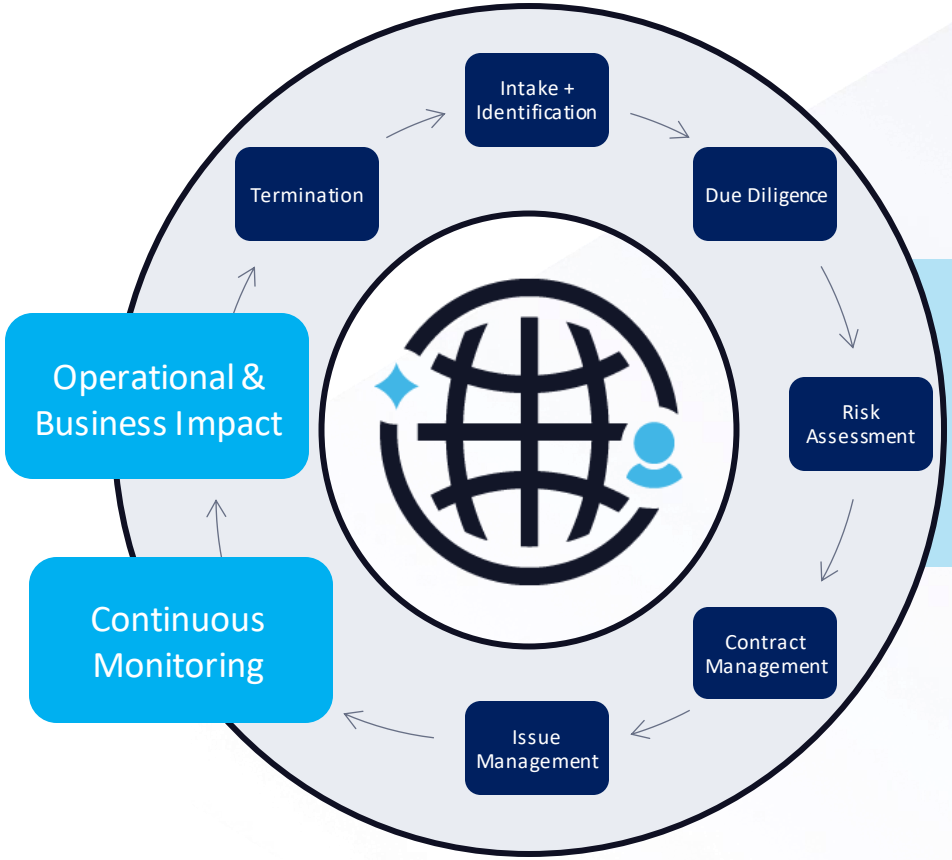
Regulatory

everbridge

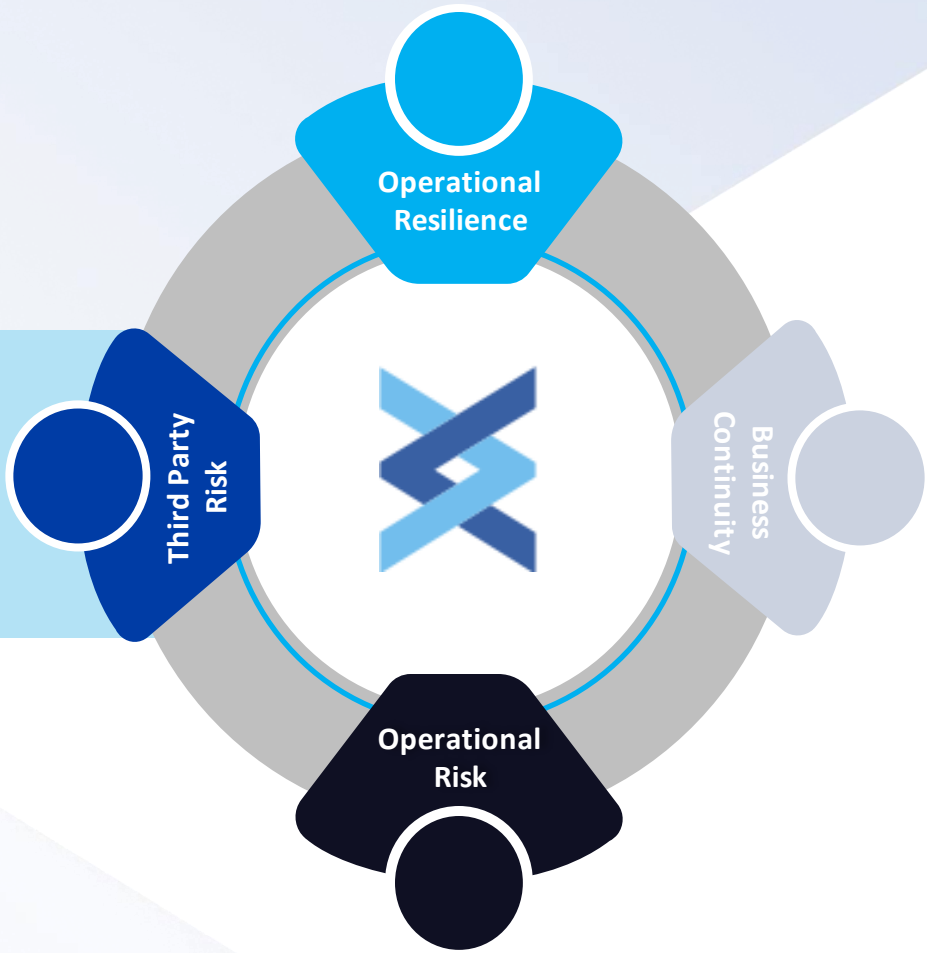
Situational Intelligence

N-party Risk Insight

Engage Third-Party Risk Teams for a Fully Cross-Functional Approach



Sharing third party risk data across disciplines enables better decisions for your business overall



Questions?

FUSION
RISK MANAGEMENT

Thank You!

Rich Cooper

Global Head of Financial Service Go-To-Market

Fusion Risk Management

Linkedin.com/in/richard-cooper/a2782b

Ryan Shea

Senior Solutions Engineer

Fusion Risk Management

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

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