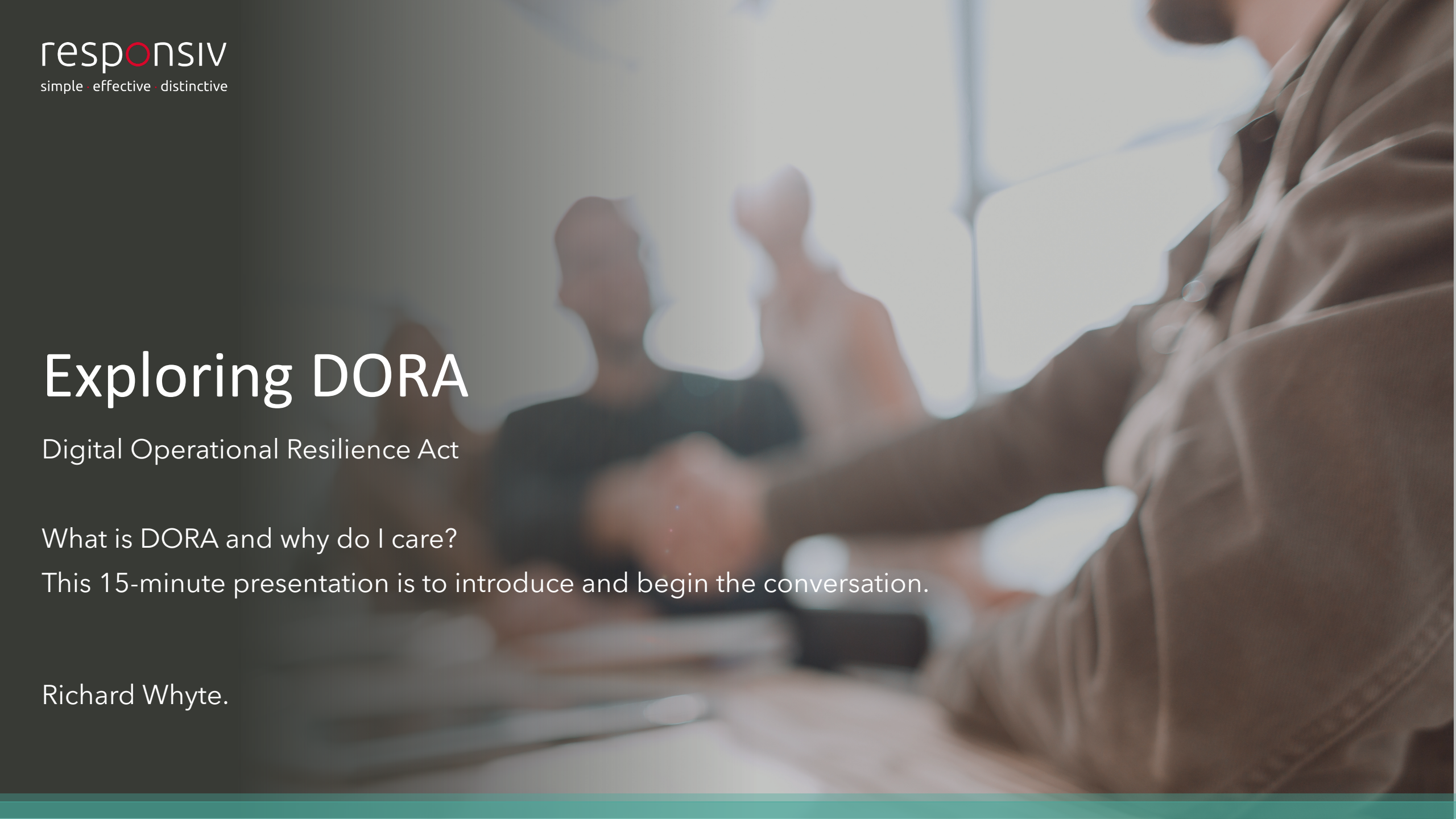
responsiv
simple · effective · distinctive



Exploring DORA

Digital Operational Resilience Act

What is DORA and why do I care?

This 15-minute presentation is to introduce and begin the conversation.

Richard Whyte.

Introduction and Disclaimer

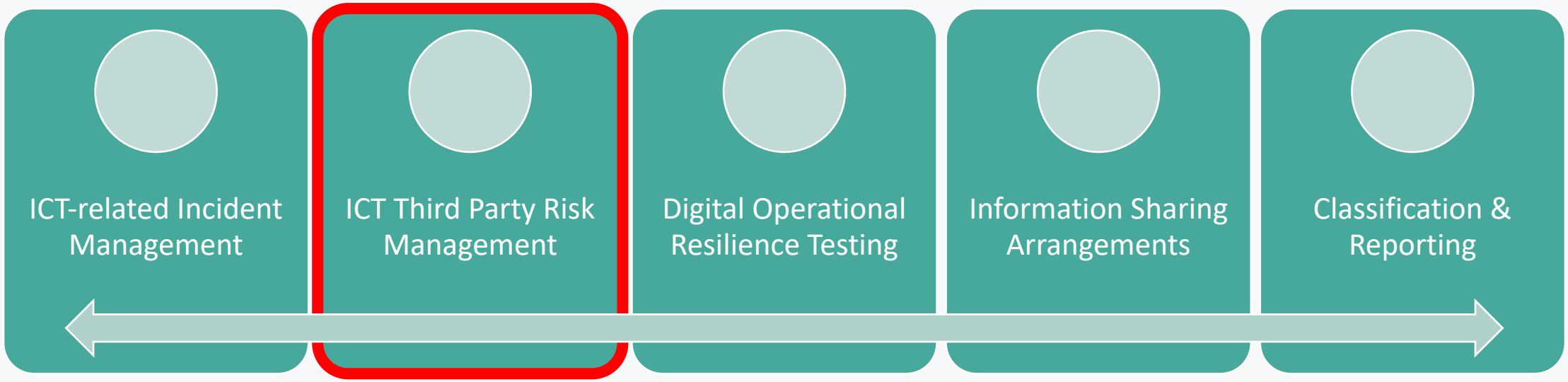
- **About me**
  - I spent ten years working for an investment bank and fifteen years in IBM before founding Responsiv
- **Responsiv**
  - Delivers cloud services and consulting to financial services companies
  - Specialists in Middleware, including API management, Integration and Process Automation
- **Disclaimer**
  - I am not legally competent to provide legal advice on DORA
- **This presentation**
  - Introduces the act
  - Considers Third-Party risk

DORA will be enforced from January 2025

2020	2022	2023	2024	2025
Draft	**Adoption**	**Entered Force**	**RTS & ITS Standards**	**Enforcement**
September 2020 EU Commission published draft DORA as part of the Digital Finance Package (DFP)	November 2022 European Parliament voted in favour and the European Council adopted DORA	January 2023 DORA entered into force and will become enforceable in 24 months…	2023 and 2024 Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) Multiple standards to be issued by ESAs.	January 2025 DORA enforceable 24 months after entry into force. Financial entities expected to be compliant with DORA.

DORA seeks convergence of **resilience** and **security** practices in financial market participants

- Builds on previous recommendations to harmonise provision of financial services
- Consistent regulatory approach to financial service participants
- Extends to **third party ICT providers** that are not participants in FS markets
- Organised in five pillars. We will focus on Third Party Risk Management



* Financial entities that have contractual arrangements for use of ICT services to run business operations **remain fully responsible** for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law. https://www.dora-info.eu/dora/article-28/

Third Party Risk

Risk to your operations originating in another party

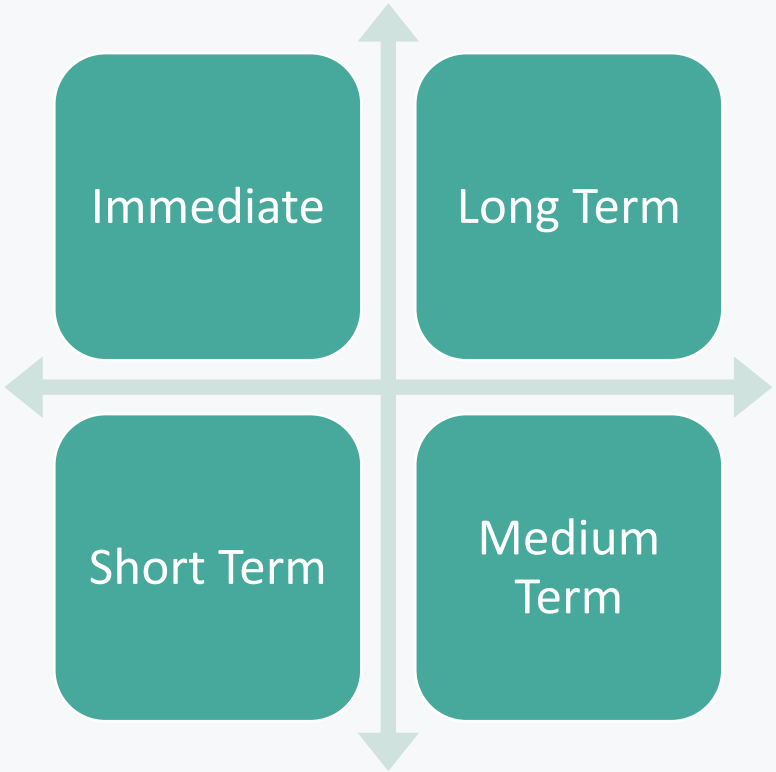
Third party event leading to	***Immediate*** *Failure*	*Strategic Failure*	*Regulatory Failure*	***Systemic*** *Failure*
An Impact to the firm causing	*Inability to operate*	*Unexpected additional cost*	*Reputational damage*	*Loss of Control or oversight*
Caused by	*Partial Failure*	*Loss of capacity*	*Loss of Oversight*	*Leading to new threats*

Third Party Risk
is like internal risks, except

- **Black Box**
  - The third-party functions until it does not
  - Third party risks tend to be invisible until they hit
  - Suggestions
    - New Contracts that require streaming metrics from the service and the right to inspect
    - Use analysis of metrics to spot trends
    - Consider the likely threats and can they be mitigated – for example with a manual or emergency process
- **Priority**
  - Will the third party prioritise your business recovery over other imperatives?
  - Can you get them to listen when there is a problem or concern?
  - Suggestion
    - Consider how to engage and escalate in the case of a problem.
    - How much control do you have and can you ask for more.
    - Exit strategies – Emergency egress, strategic withdrawal
- **Recovery**
  - You are relying on the third party to recover the situation. Do they have the skills?
  - Is there data or function that is unique to the service, or can it be duplicated with standby?
  - Suggestion
    - Consider how to maintain ***functional*** access to your data in the event of a problem

Risk Evaluation:
Threat and Error Management (TEM)

- **Threats** are external events with potential to disrupt operational integrity
  - Response to threats determines the possibility of errors
  - Categorised by
    - Degradation of operations
    - Immediacy
    - Scope
    - Cost
- **Errors** are mistakes made by people responding to Threats
  - Can make things worse and responsible for more non-availability than threats
  - Errors undermine response and must be included in planning



Methodology

Scope of work

- Identify processes in scope for DORA.
- Identify systems, infrastructure, people, data.
- Identify directly involved Critical Third Parties

Peripheral dependencies

- Security, certificates, passwords
- Networks and premises
- Third parties that support, provide, operate

Threat impact and priority

- Identify critical threats
- Assess impact (Immediate, Short, Medium, Long Term)
- Identify Systemic Threats that Impact multiple systems (Cloud Hosting)

Plan

- Prioritise based on threat
- Plan responses to each of the threats document potential errors in the response.
- Document Response policies for types of threat

Respond

- Establish processes and working practices to minimise risk.
- Instigate regular testing
- Engage third parties to establish a joint response.

To Conclude

DORA transcends traditional infrastructure concerns to focus on continuity of business services.

It encompasses reporting, control, monitoring, governance, and the identification and management of risks.

This holistic approach recognises that operational resilience is multifaceted, demanding more than just robust systems; it requires processes that can sustain business functions under duress.

- The number of systems needed to operate a business long term is high
- The number of systems needed to operate in the immediate term for 90% of the business is much smaller

- Focus attention on the few systems and threats that can cause immediate problems
- Develop a framework/structured approach to maintain focus and control of the DORA project

responsiv
simple · effective · distinctive

Any Questions

Richard Whyte

information@responsiv.co.uk

responsiv.co.uk

Responsiv

@BeingResponsiv