The Trustee's Perspective

DORA and the Register of Information

Shane Coman (CEO & Founder)

nexus assurance

Overview

- The Digital Operational Resilience Act, or DORA, is aimed at strengthening the digital operational resilience of financial entities.

- DORA's primary objective is to ensure that financial institutions can withstand, respond to, and recover from all types of ICT-related disruptions and threats.

- What Pension Schemes are in scope? (The pensions authority)

    - Schemes with 100 or more active and deferred members are subject to all DORA requirements.

    - Schemes with 16-99 active and deferred members are subject to most of the DORA requirements. However, a simplified version of the ICT risk management framework applies for these schemes, and they are exempt from performing advanced testing of ICT systems and from having to adopt a strategy on ICT third-party risk.

    - Schemes with 15 or less active and deferred members are not subject to DORA.

- The go-live date for the application of these standards is January 17, 2025.

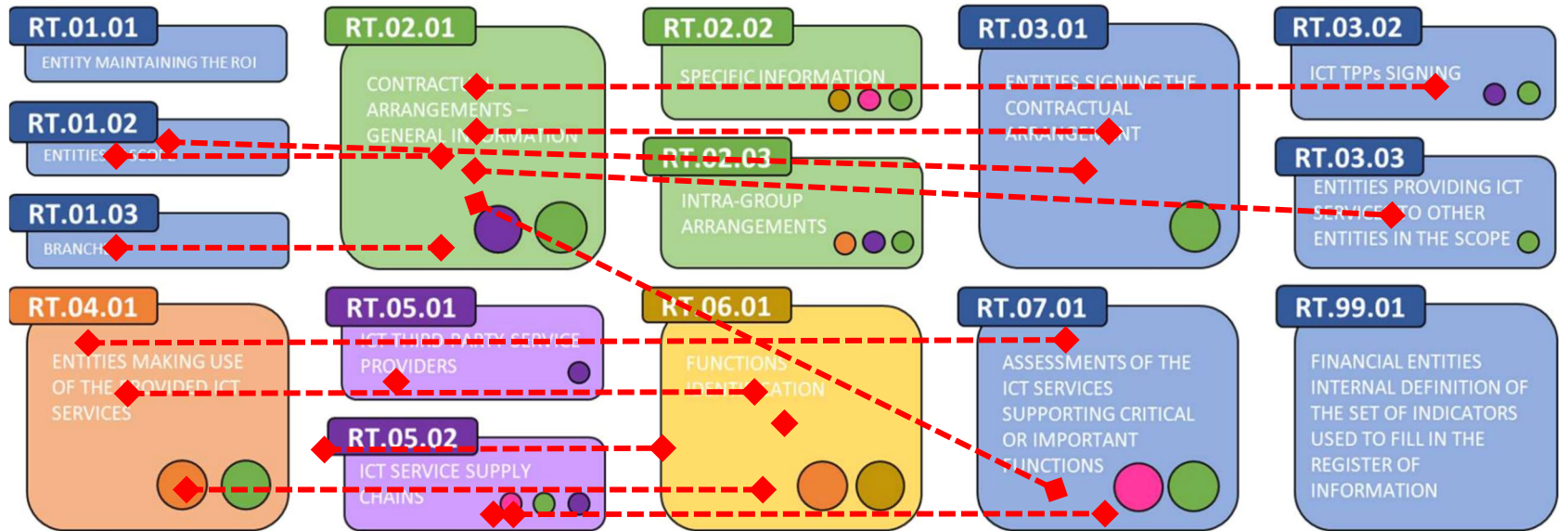- The Register of Information obligation is driven by legislation (not guidance)!

The Register of Information

- As part of the ICT risk management framework, all entities in scope must create, maintain and submit a Register of Information regarding all contractual arrangements on the use of ICT services provided by ICT third-party service providers.

- Some context - Why?

  - **Financial Entities** (FEs) should maintain sound monitoring of ICT third-party risk. The ICT third-party risk strategy adopted by the <u>management bodies</u> of FEs should be "rooted in a continuous screening of all ICT third-party dependencies".

  - **Competent Authorities** (CAs) need to enhance their supervisory awareness and engage in effective supervision of FEs' ICT third-party dependencies

  - **The European Supervisory Authorities** (ESAs) with the help of CAs will initiate an oversight framework to identify and oversee critical ICT third-party service providers.

- Timing:

  - Schemes are obligated to have a complete Register of Information in place by January 17th 2025.

  - CAs can request your register for supervision purposes at any time after Jan 17th 2025.

The Register of Information is Complicated

- The register of information is composed of 15 templates. Across the templates there are 105 data point to be entered. The expected interconnectivity of data point plus the depth of data required will present a challenge for schemes.

Illustration 1: Structure of the Register of Information

Tips for Trustees

- **Get Started:** Ensure that schemes in scope have a Register of Information project.

- **Who:** Figure out who is taking *responsibility* for this project.

- **Recognise as an ongoing obligation:** The Register of Information will have a life well beyond January 17th, 2024. Ask how the scheme intends to maintain this complex register. Key person risk should be considered.

- **Criticality:** Ask about your function criticality assessment. It is a foundation data point for DORA so it needs to be ready or planned.

- **Board access and oversight:** One of the objectives of the Register is to provider a firm with a toolkit to oversee ICT third party providers. Ask how the board will get access to a summary of the register to support their oversight.

- **Mapping and Submission:** Ask how the scheme will map, codify and submit the register.

- **Do Not Underestimate:** For schemes this is a complex exercise. Find out if your scheme thinks the same. If not, go deeper.