Information Sharing Arrangements

*Part 5 of the **DORA Deep Dive** Series*

Presented By:

Gerard Joyce, CTO, CalQRisk

Fiona Kiely, Snr Research Analyst, CalQRisk

Tuesday 14th December 2024

Outline

- Introduction
- DORA Overview
- Summary of ESAs Workshop on DORA Dry Run Lessons Learnt
- Information Sharing Arrangements (What's in the Act)
- Concerns
- Why Share
- How to Share
- Q&A

Who we are and what we do

- Experienced Risk & Compliance Professionals
- Members of IRM, IOB, CI (ACOI), IoD, ACCA, ISACA, ….
- We Make A Governance, Risk & Compliance Solution called CalQRisk
  - A cloud-based software solution
  - Includes a DORA-specific solution (Checklists / Register of Information report..)
- Risk Advisory Service
  - In-house / Virtual Training, Strategic Risk Alignment, Risk Management Framework development
- CalQRisk is used by 4,000+ users in regulated firms and others

  Including: Financial Services organisations and Not-For-Profit sector / Public Sector

66

Everyone needs help from everyone

Bertolt Brecht

The miracle is this: The more we share the more we have

Leonard Nimroy (Spock)

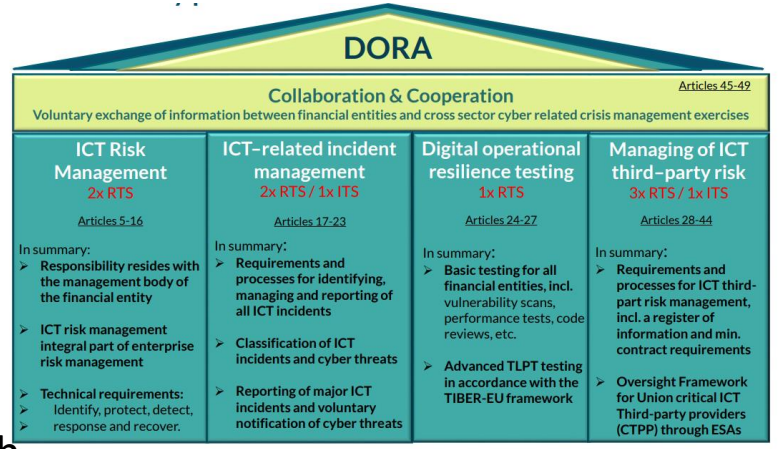
99

DORA Overview

- A Regulation. Applies to all EU Member States
- Came into force in Jan 2023
- It becomes applicable on Jan 17th 2025…. **This week!**
- Applies to financial entities and some of their service providers
- It's about making the ICT systems that support financial business better
- Better in the sense that they are more secure, less likely to fail, faster to get back up and running, if they do fail.
- It harmonises and improves several guidelines that are in operation today.

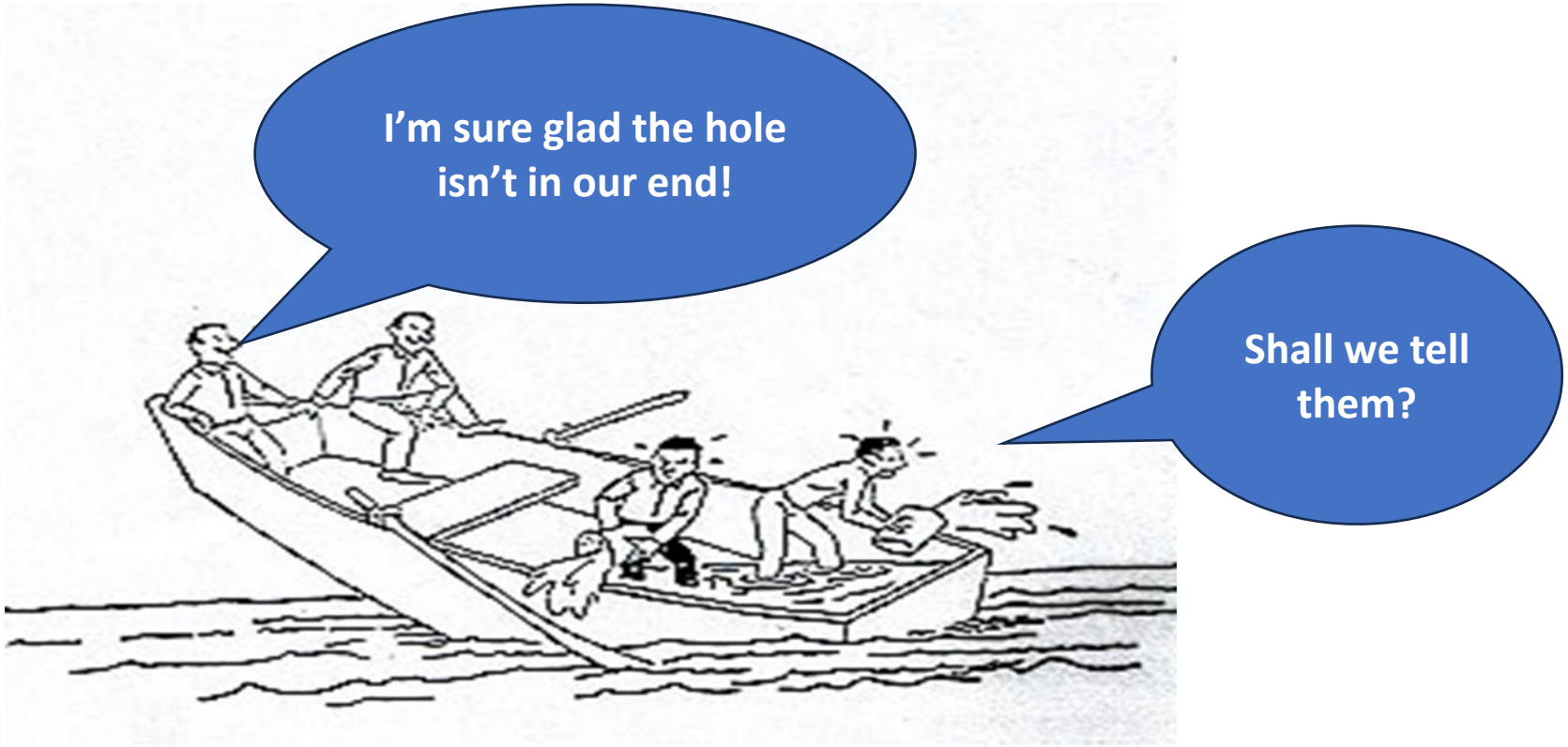
DORA closes a gap by ensuring that operational resilience is not merely about financial buffers

DORA Five Pillars



- ICT Risk Management Framework - Oct 15th
- ICT Third Party Risk Management - Nov 12th
- ICT-related Incident Management - Nov 26th
- Digital Operational Resilience Testing - Dec 10th
- **Information Sharing Arrangements- Jan 14th Today**

Interdependency



ESAs DORA Workshop Dec 18

- The EBA conduct 116 “Quality Checks” on the data and the submission will be rejected if it fails these tests. (See “Draft validation rules for DORA reporting of RoI”)
- A Blank field where mandatory data is expected was the most common failure
- Provision of ID codes for Third Parties and their parents seemed “problematic”
- Only 6.5% did not fail any quality check in the Dry Run. “The instructions in the ITS must be adhered to”
- EUID is now an acceptable alternative to LEI for Third Party identification code.
- LEI is the ONLY acceptable identifier for financial entities.
- Expired contracts are no longer required to be in the register.

ESAs DORA Workshop Dec 18 ctd

- Register is to be submitted in plain-csv files in a ZIP file. (Do not submit in Excel)
- Financial entities were encouraged to maintain the registers in an appropriate tool (not Excel, due to the relational nature of the information).
- All functions (services) that have a dependency on an ICT Third Party must be included in the register, whether critical or not. (this may impact their consideration of who is a CTPP)
- ESA expect submissions from Competent Authorities by 30th April 2025
- The various CAs will set their own deadlines, the most common being 31st March 2025
- A “Technical Package” with all the detailed instructions / requirements / taxonomy was made available. See. https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

DORA Register of Information

Text version

c0010	c0020	c0030	c0040	c0050	c0060	c0070	c0080	c0090	c0100	c0110	c0120
Identification code of the ICT third-party service porvider	Type of code	Additional code of ICT third-party serice provider	Type of addional code	Name of ICT third-party service provider	Name of ICT third-party service provider in Latin alphabet	Type of person of the ICT third-party service provider	Country of the ICT third-party service provider's headquarters	Currency	Estimated cost of the ICT third-party service provider	Identification code of the ICT third-party service provider's ultimat parent undertaking	Type of Code
12345678901234567890	LEI	EUcodehere12345	EUID	IT Service Provider Ltd	IT Service Provider Ltd	Legal person, excluding individual acting in a business capacity	US	Euro	3457	Par123000xxx000	LEI
620051	CRN			Sample Contractor	Sample Contractor	Legal person, excluding individual acting in a business capacity	GB	US Dollar	56789	Par234000yyy000	Missing!
Missing!	Missing!			Network Services	Network Services	Missing!	Missing!		0		
SSP123456789-on92	LEI			NexaCorp Solutions	NexaCorp Solutions	Legal person, excluding individual acting in a business capacity	AL		0		
3099999	LEI	9876543210	Missing!	ACME Limited	ACME Limited	Legal person, excluding individual acting in a business capacity	US	Pound Sterling	4568		
Missing!	Missing!			DOT Limited	DOT Limited	Missing!	FR		0		
9876543210	CRN			ABC Shared Services	ABC Shared Services	Missing!	US	Euro	Missing!		
12345678901234567890	LEI	EUcodehere12345	EUID	IT Service Provider Ltd	IT Service Provider Ltd	Legal person, excluding individual acting in a business capacity	US	Euro	3457	Par123000xxx000	Missing Separator
Missing!	Missing!			Software Developers Inc	Software Developers Inc	Legal person, excluding individual acting in a business capacity	Missing!		Missing!		

Information Sharing Arrangements (Act- Ch VI)

Recital 32

- With ICT risk becoming more and more complex and sophisticated, good measures for the detection and prevention of ICT risk depend to a great extent on the regular sharing between financial entities of threat and vulnerability intelligence. Information sharing contributes to creating increased awareness of cyber threats. In turn, this enhances the capacity of financial entities to prevent cyber threats from becoming real ICT-related incidents and enables financial entities to more effectively contain the impact of ICT-related incidents and to recover faster. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, in particular uncertainty about its compatibility with data protection, anti-trust and liability rules.

Recital 34 …

- Financial entities should be encouraged to exchange among themselves cyber threat information and intelligence, …. Those mechanisms should comply with the applicable competition law rules of the Union set out in the Communication from the Commission of 14 January 2011entitled 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements …. And GDPR

Information Sharing Arrangements (Act- Ch VI)

- **Article 45: Information-sharing arrangements on cyber threat information and intelligence**
- Financial Entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools
- Information-sharing must:
  - Be carried out within a trusted group with the aim of strengthening digital operational resilience (of the sector)
  - Ensure the protection of sensitive information
  - Adhere to business confidentiality and data protection laws
  - Define the conditions for participation.
- Where appropriate, these arrangements must set out details on:
  - The involvement of public authorities and the capacity in which they may be associated to the arrangements.
  - The involvement of ICT third-party service providers, and
  - Operational elements, including the use of dedicated IT platforms.
- Financial entities must notify their respective competent authorities once their membership in an information-sharing arrangement is validated, and when their membership ceases.

Information Sharing Concerns

- Sensitive Information being shared with potential competitors
  - Protect sensitive information
  - Have rules of conduct
- GDPR
  - Treat any personal data share as you would in any other operational capacity.

When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Why Share?

- The risks affect the entire financial system
- Everyone benefits from the collective intelligence.. collective resilience
- Earlier Awareness – Earlier response
- The bad guys collaborate, so why not the good guys!

How to Share?

- Information Sharing networks / groups
- Share anonymised / pseudo-anonymised data
- Participate in cyber threat intelligence platforms
- Receive aggregated / anonymised information on incidents from the regulator
- Engage / collaborate with the NCSC (Irl / UK)
- Don’t forget to share internally too… across all departments

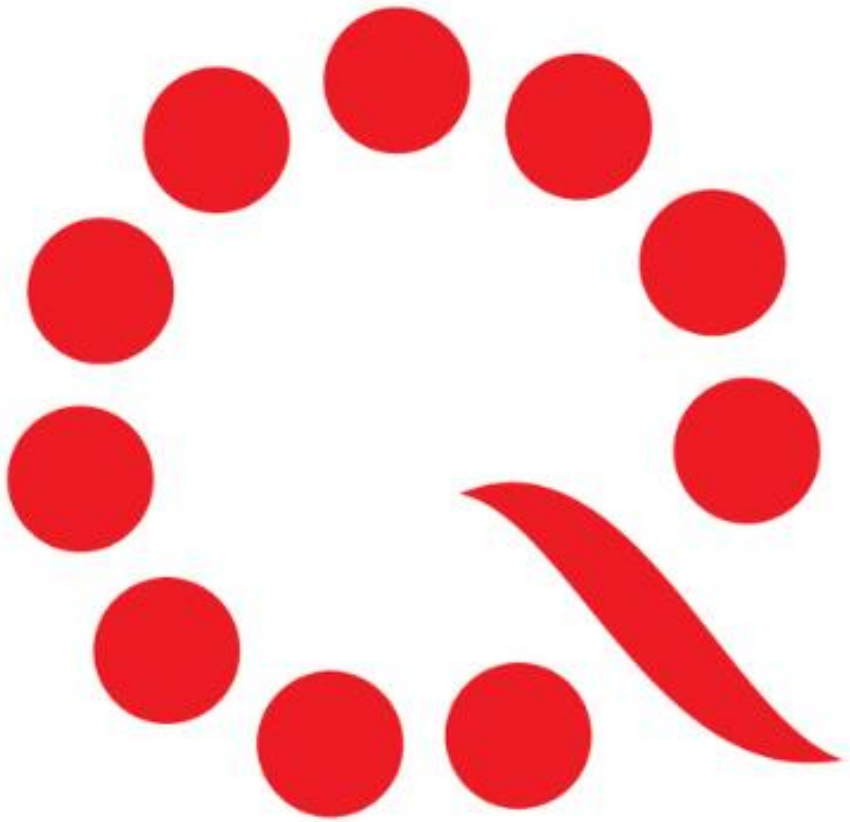
Information Sharing Arrangements

Some Organisations

FS-ISAC	**https://www.fsisac.com/**
NCCGroup	**https://www.nccgroupplc.com/**

Takeaways

- Read Article 45
  - Speak with your counterparts in other organisations and find out if an appropriate information-sharing organisation exists, or do you need to form one
- Keep aware of what threats and vulnerabilities apply to you
  - Gather Threat Intelligence, act on it, share what you can
- Just 3 days to go!



Questions ?

gerard.joyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk