ICT Third Party Risk Management

*Part 2 of the **DORA Deep Dive** Series*

Presented By:

Gerard Joyce, CTO, CalQRisk

Tuesday 12th November 2024

Outline

- Introductions
- DORA Overview
- ICT Third Party Risk Management (What's in the Act)
- Regulatory Technical Standards (2024/1773)
- Register of Information
- Q&A

Who we are and what we do

CalQRisk

- 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 3,000+ users in regulated firms and others

  Including: Financial Services organisations and Not-For-Profit sector: Housing Associations, Charities, Sports Organisations

> I can do things you cannot, you can do things I cannot; together we can do great things
>
> *Mother Teresa*

DORA Overview

- A Regulation. Applies to all EU Member States
- Came into force in Jan 2023
- It becomes applicable on Jan 17th 2025
- 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 Today
- ICT-related Incident Management - Nov 26th
- Digital Operational Resilience Testing - Dec 10th
- Information Sharing Arrangements- Jan 14th

ICT Third Party Risk Management (Act)

- **Article 5**: Governance and organisation (policy on arrangements, responsibilities, reporting)
- **Article 6**: ICT risk management framework (policies, protocols, multi-vendor strategy, rationale, OR strategy, objectives, review)
- **Article 8**: Identification (dependent processes, interconnections)
- **Article 11**: Response and recovery (BC plans, BIA)
- **Article 26:** Advanced testing of ICT tools, systems and processes based on TLPT (identify, participation)
- **Article 28:** General Principles (manage third-party risk, register of information, contractual arrangements, exit)
- **Article 29:** Preliminary assessment of ICT concentration risk at entity level (multiple contractual arrangements)
- **Article 30:** Key contractual provisions (rights and obligations, functions, locations, information security, SLA, cooperation, termination, awareness prog, notice, BC plans, performance monitoring, exit strategies)

ICT Risk Management

The How

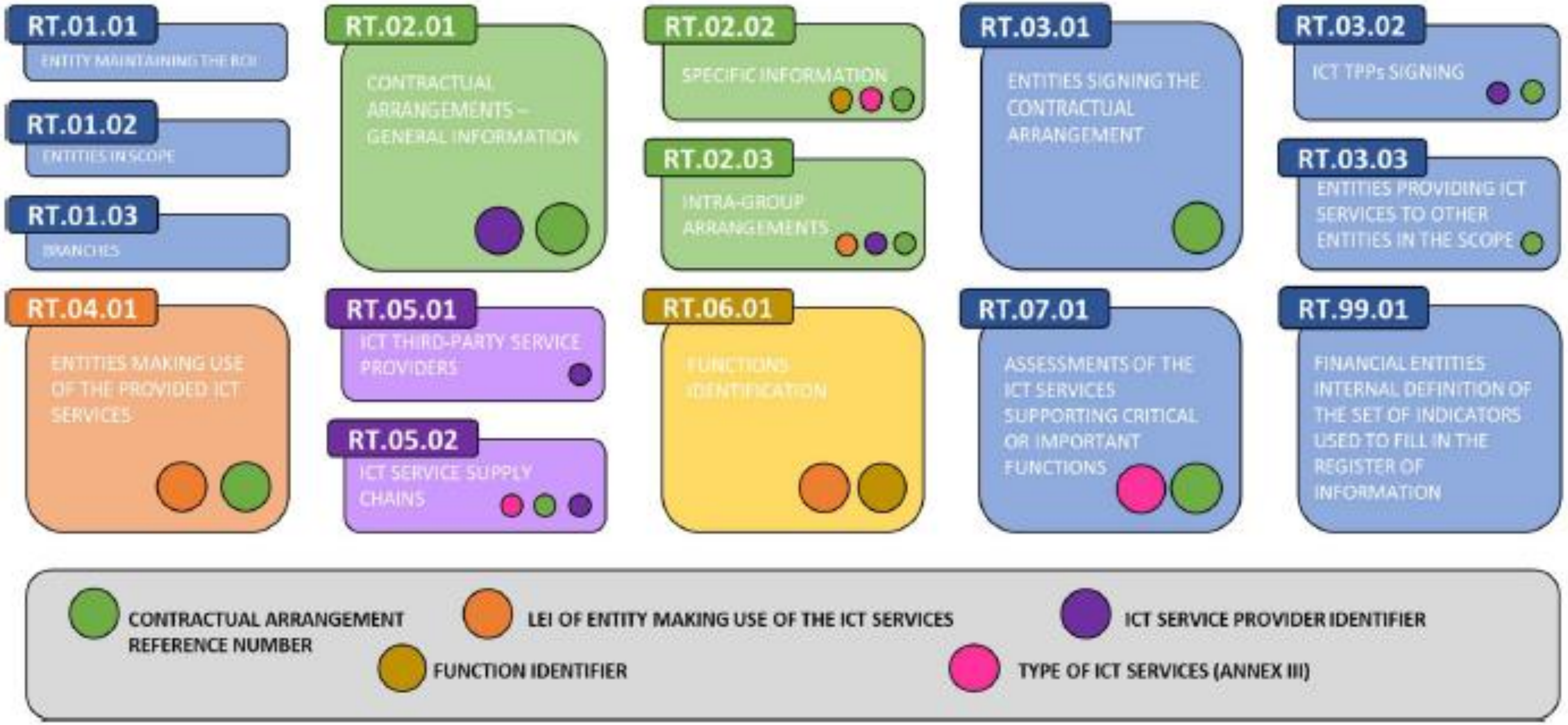
Regulatory Technical Standards (RTS 2024/1773)

- **Article 1**: Overall risk profile and complexity
  - (policy, type of service, location, data, intra-group, regulated, EU/not, concentration, transfer, disruption)
- **Article 2**: Group application (parent responsible for consistent implementation)
- **Article 3**: Governance arrangements
  - (update annually, methodology, responsibilities, resources, reporting, contractual arr consistent with other policies. Reqs, indep review)
- **Article 4**: Main phases of the life cycle for the adoption and use of contractual arrangements
  - (decision-making, RA/DD, controls, management, register of information, exit strategies)
- **Article 5**: Ex-ante risk assessment (needs, risk assessment-several areas)
- **Article 6**: Due diligence
  - (reputation, ability, resources, info sec, sub-contractors, where data stored, can audit, ethics, RM/BC, DD process, performance)
- **Article 7**: Conflicts of interest (identify, prevent, manage, intra-group-objective decision-making)
- **Article 8:** Contractual clauses (written, audits, methods, document changes)
- **Article 9**: Monitoring of the contractual arrangements (performance, compliance, reports, audits, incident notification, shortcomings)
- **Article 10:** Exit from and termination of the contractual arrangements (policy to require Exit plan, various scenarios)

ITS for Register of Information

- DORA mandates the European Supervisory Authorities (ESAs) to develop **implementing technical standards (ITS)** to establish the standard templates for the purposes of the register of information
- The standard templates of the register of information are proportionate by design. *The more TPs you have the bigger the register.*
- The draft ITS proposes a single set of templates that is common to all financial entities, subgroup and group to be used to report information in the Register of Information.
- Supports the continuous screening of all ICT third-party dependencies.

ITS for Register of Information - Structure



RT.01.01 ENTITY MAINTAINING THE ROI

RT.01.02 ENTITIES IN SCOPE

RT.01.03 BRANCHES

RT.02.01 CONTRACTUAL ARRANGEMENTS – GENERAL INFORMATION

RT.02.02 SPECIFIC INFORMATION

RT.02.03 INTRA-GROUP ARRANGEMENTS

RT.03.01 ENTITIES SIGNING THE CONTRACTUAL ARRANGEMENT

RT.03.02 ICT TPPs SIGNING

RT.03.03 ENTITIES PROVIDING ICT SERVICES TO OTHER ENTITIES IN THE SCOPE

RT.04.01 ENTITIES MAKING USE OF THE PROVIDED ICT SERVICES

RT.05.01 ICT THIRD-PARTY SERVICE PROVIDERS

RT.05.02 ICT SERVICE SUPPLY CHAINS

RT.06.01 FUNCTIONS IDENTIFICATION

RT.07.01 ASSESSMENTS OF THE ICT SERVICES SUPPORTING CRITICAL OR IMPORTANT FUNCTIONS

RT.99.01 FINANCIAL ENTITIES INTERNAL DEFINITION OF THE SET OF INDICATORS USED TO FILL IN THE REGISTER OF INFORMATION

- ● CONTRACTUAL ARRANGEMENT REFERENCE NUMBER
- ● LEI OF ENTITY MAKING USE OF THE ICT SERVICES
- ● ICT SERVICE PROVIDER IDENTIFIER
- ● FUNCTION IDENTIFIER
- ● TYPE OF ICT SERVICES (ANNEX III)

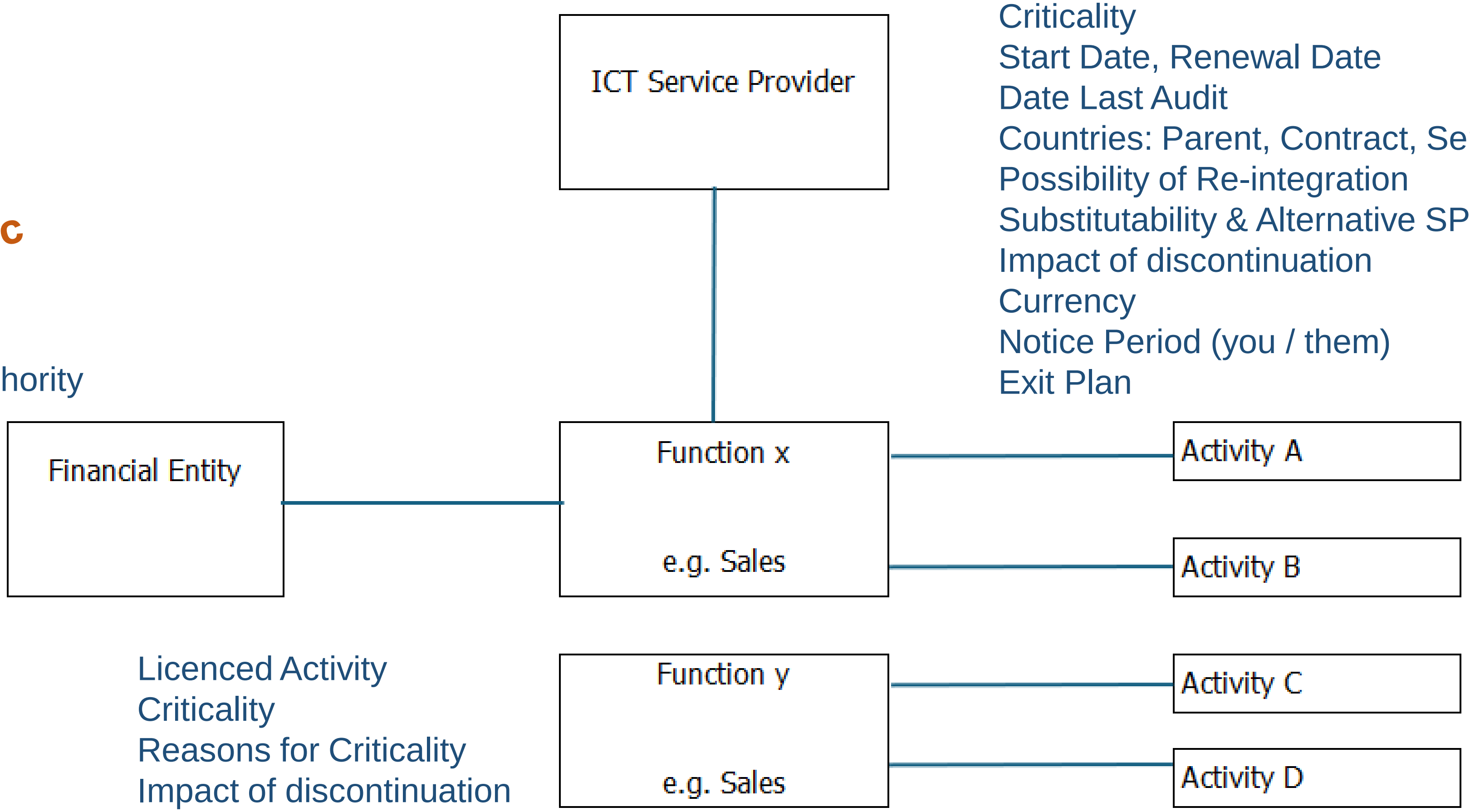
What needs to be included?

Sample

Identification Code
Name
Category of service provided
Criticality
Start Date, Renewal Date
Date Last Audit
Countries: Parent, Contract, Service, Data Stored
Possibility of Re-integration
Substitutability & Alternative SPs
Impact of discontinuation
Currency
Notice Period (you / them)
Exit Plan

Static

LEI
Name
Country
Competent Authority



ICT Service Provider

Financial Entity

Function x

e.g. Sales

Function y

e.g. Sales

Activity A

Activity B

Activity C

Activity D

Licenced Activity
Criticality
Reasons for Criticality
Impact of discontinuation
Sensitivity of data stored
Level of reliance on the ICT service

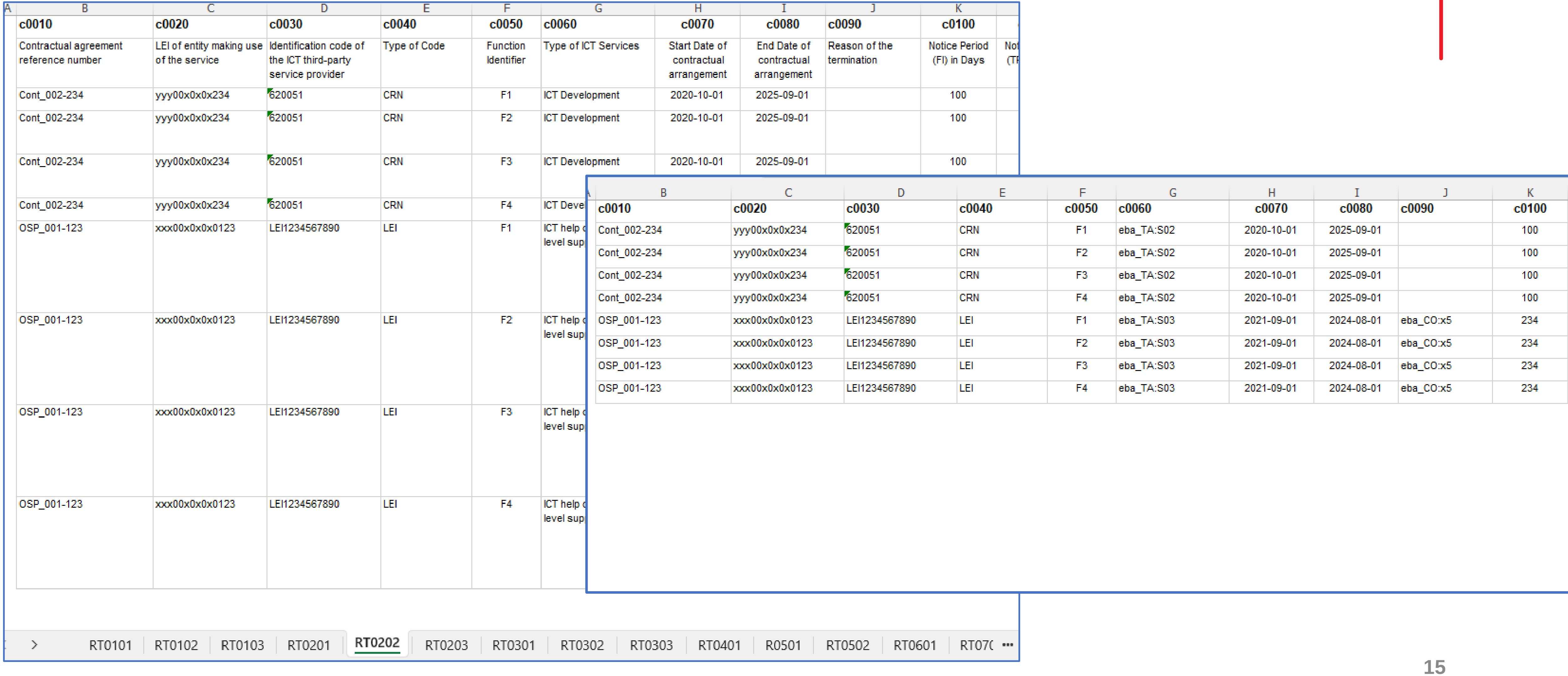
ITS for Register of Information - Templates

- RT.01.01 Entity Maintaining the ROI *
- RT.01.02 Entities in Scope *
- RT.01.03 List of Branches *
- RT.02.01 Contractual Arrangements – General Information
- RT.02.02 Contractual arrangements – Specific Information
- RT.02.03 Contractual arrangements – Intra-group *
- RT.03.01 Entities signing the contractual arrangements *
- RT.03.02 ICT TPs signing the contractual arrangements
- RT.03.03 Entities providing ICT Services to other entities in the scope *

ITS for Register of Information - Templates ctd

- RT.04.01 Entities making us of the provided ICT services *
- RT.05.01 ICT Third-Party service providers
- RT.05.02 ICT service supply chains
- RT.06.01 Functions identification
- RT.07.01 Assessment of the ICT services
- RT.99.01 FE definitions of the set of indicators used to fill in the RoI *

ITS for Register of Information - Report



B	C	D	E	F	G	H	I	J	K
c0010	c0020	c0030	c0040	c0050	c0060	c0070	c0080	c0090	c0100
Contractual agreement reference number	LEI of entity making use of the service	Identification code of the ICT third-party service provider	Type of Code	Function Identifier	Type of ICT Services	Start Date of contractual arrangement	End Date of contractual arrangement	Reason of the termination	Notice Period (FI) in Days
Cont_002-234	yyy00x0x0x234	620051	CRN	F1	ICT Development	2020-10-01	2025-09-01		100
Cont_002-234	yyy00x0x0x234	620051	CRN	F2	ICT Development	2020-10-01	2025-09-01		100
Cont_002-234	yyy00x0x0x234	620051	CRN	F3	ICT Development	2020-10-01	2025-09-01		100
Cont_002-234	yyy00x0x0x234	620051	CRN	F4	ICT Devel				
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F1	ICT help d level sup				
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F2	ICT help d level sup				
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F3	ICT help d level sup				
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F4	ICT help d level sup				

RT0101 RT0102 RT0103 RT0201 RT0202 RT0203 RT0301 RT0302 RT0303 RT0401 R0501 RT0502 RT0601 RT07(...

B	C	D	E	F	G	H	I	J	K
c0010	c0020	c0030	c0040	c0050	c0060	c0070	c0080	c0090	c0100
Cont_002-234	yyy00x0x0x234	620051	CRN	F1	eba_TA:S02	2020-10-01	2025-09-01		100
Cont_002-234	yyy00x0x0x234	620051	CRN	F2	eba_TA:S02	2020-10-01	2025-09-01		100
Cont_002-234	yyy00x0x0x234	620051	CRN	F3	eba_TA:S02	2020-10-01	2025-09-01		100
Cont_002-234	yyy00x0x0x234	620051	CRN	F4	eba_TA:S02	2020-10-01	2025-09-01		100
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F1	eba_TA:S03	2021-09-01	2024-08-01	eba_CO:x5	234
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F2	eba_TA:S03	2021-09-01	2024-08-01	eba_CO:x5	234
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F3	eba_TA:S03	2021-09-01	2024-08-01	eba_CO:x5	234
OSP_001-123	xxx00x0x0x0123	LEI1234567890	LEI	F4	eba_TA:S03	2021-09-01	2024-08-01	eba_CO:x5	234

Takeaways

- Make sure you have a robust contract template
- Identify all your third-parties now and what information you have
- Identify which are the critical ones and focus on them
- Identify the critical services (functions) you deliver and focus on them
- Only 2 months to go (to Jan 17 2025) !!

Questions ?

gerard.joyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk