

DORA Chapter V Decoded

Building a Bulletproof Third-Party Risk Framework

Bastiaan Bruyndonckx
Partner

Today's Agenda

- A. Setting the Scene
- B. Key Concepts Decoded
- C. Governance Backbone
- D. Pre-Contractual Risk Analysis
- E. Contractual Safeguards
- F. Exit Strategies & Ongoing Monitoring
- G. Subcontracting Chains & ICT Concentration Risk
- H. CTPP Oversight Framework
- I. Key Takeaways

A. Setting the Scene

Why Chapter V? DORA in Context

-  **Growing dependency on external ICT providers**
 - Cloud providers · Software suppliers · Data analytics · Hardware-as-a-service
 - A single provider failure can cascade across the entire financial system
-  **DORA's five-pillar architecture**
 - ICT risk management · Incident reporting · Resilience testing · Information sharing · Third-party risk (Ch. V)
-  **Chapter V governs the full outsourcing lifecycle**
 - Strategy → Pre-contractual → Contract → Monitoring → Exit
-  **The numbers confirm the risk — ESA Joint ICT Incidents Report, 2025**
 - 3,383 major ICT-related incidents reported across the financial sector in 2025
 - 51% were system failures, **almost 1 in 3 traced back to a third-party provider failure**

B. Key Concepts Decoded



Key Concepts (1/2)



- **ICT services**
 - *"**digital and data services** provided through **ICT systems** to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services"*
 - E.g. cloud computing, software, data analytics, data centre services...
- **ICT third-party risk**
 - *"**ICT risk** that may arise for a financial entity in relation to its **use of ICT services** provided by **ICT third-party service providers** or by **subcontractors** of the latter, **including** through **outsourcing arrangements**"*
- **ICT risk**
 - *"any reasonably identifiable **circumstance** in relation to the use of network and information systems which, **if materialised, may compromise the security of the network and information systems**, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment"*



Key Concepts (2/2)



- **Proportionality**

- *“In addition, the application by financial entities of Chapters III, IV and V, Section I [= ICT third-party risk management], shall be **proportionate** to their **size and overall risk profile**, and to the **nature, scale and complexity of their services, activities and operations**, as specifically provided for in the relevant rules of those Chapters.”*

- **Critical or important function (CIF)**

- *“a function, the disruption of which would **materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities**, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law”*

- **CIF classification is the pivotal threshold**

- It determines the enhanced tier of obligations at every stage of the outsourcing lifecycle
- Methodology must be formalised, documented and periodically reviewed (RTS 2024/1773)

C. Governance Backbone

Governance: Strategy & ICT Third-Party Officer



- **Full responsibility remains with the financial entity - always**
 - Outsourcing does not transfer regulatory responsibility
- **ICT Third-Party Risk Strategy (Art. 28(2))**
 - Adopted and regularly reviewed by the management body
 - Includes a policy on ICT services supporting CIFs → RTS 2024/1773
 - Multi-vendor strategy to be considered where applicable
 - Applied at individual, sub-consolidated and consolidated level
- **ICT Third-Party Officer**
 - Designated senior management role
 - Oversees all third-party arrangements · Reports to management body on risk exposure
- **Management body**
 - Regular review of risks arising from CIF contractual arrangements

RTS 2024/1773: The Policy on ICT services supporting CIFs in Practice



- **Formal CIF policy — adopted and reviewed at least annually by the management body**
- **Covers the full contractual lifecycle in 6 steps:**
 - ① Planning → ② Risk assessment → ③ Due diligence
 - ④ Contracting → ⑤ Monitoring → ⑥ Exit
- **Due diligence content (Art. 6 RTS 2024/1773)**
 - Business reputation · Financial/human/technical resources · Information security
 - Regulatory status · Third-country location · ESG criteria
- **Audit rules**
 - ✗ Cannot rely solely on certifications or third-party audit reports over time
 - ✓ Direct audit rights must always be preserved and exercised
 - ✓ Pooled audits with other contracting entities are permitted
- **CIF arrangements must be included in the internal audit plan + independent review**

Register of Information: Core Obligations (Art. 28(3))

Obligation	Key requirements
Register content	All ICT contractual arrangements · Clear distinction CIF vs non-CIF Maintained at entity, sub-consolidated and consolidated level
Regulatory access	Full register (or specified sections) available to competent authority on request
Annual reporting	Number of new arrangements · Categories of providers · Type of arrangements · ICT services and functions provided
Prior notification	Inform regulator before entering into a planned CIF arrangement Notify when an existing function becomes critical or important

ITS 2024/2956: Standardised Register Templates in Practice



Template	Content
B_01.01 / 01.02	Financial entity & branch identification
B_02.01 / 02.02	Contractual arrangements — general information & ICT service details
B_03.01 / 03.02	Entities signing arrangements · ICT providers signing for services
B_05.01 / 05.02	ICT provider identification + full ICT service supply chain (ranking: rank 1 = direct provider)
B_06.01	Function identification — LEI + licensed activity + function → unique function identifier
B_07.01	CIF risk assessment — substitutability, date of last audit, impact of discontinuation
B_99.01	Definitions used by financial entity (e.g., meaning of low/medium/high impact)



Mandatory identifiers: LEI or EUID for all legal persons supporting CIFs · Data quality: accuracy · completeness · consistency · integrity · uniformity · validity · Groups: one register for all levels is sufficient

D. Pre-Contractual Risk Analysis

Pre-Contractual Risk Analysis: General Requirements (Art. 28(4)–(5))



- **Mandatory pre-contractual gate - must be completed before signing any ICT contract**
- **5 steps required:**
 - ① Assess whether the service supports a CIF
 - ② Verify whether supervisory conditions for contracting are met
 - ③ Risk assessment: operational · legal · ICT · reputational · data protection · ICT concentration risk
 - ④ Due diligence on prospective provider: capabilities, financial soundness, information security
For CIF → most up-to-date and highest quality information security standards required
 - ⑤ Identify and manage conflicts of interest (incl. intra-group — pricing must be objective)

Pre-Contractual Risk Analysis: CIF-Specific Assessments (Art. 29)



- **1. ICT concentration risk**
 - Is the provider easily substitutable? (market share · proprietary tech · migration cost)
 - Multiple CIF arrangements stacked on the same or closely connected providers?
- **2. Subcontracting chain analysis**
 - Length and complexity of chain
 - Impact on ability to monitor functions and regulator's ability to supervise the entity
- **3. Third-country provider considerations**
 - Union data protection compliance
 - Effective enforcement of applicable law in the provider's jurisdiction
- **4. Insolvency law risks**
 - What happens to data if the provider becomes insolvent?
 - Constraints on urgent data recovery in a bankruptcy scenario

E. Contractual Safeguards

Art. 30 DORA: A Two-Tier Contractual Framework

	Art. 30(2) — All ICT contracts	Art. 30(3) — CIF contracts only
Scope	Every written ICT service arrangement	Arrangements supporting Critical or Important Functions
Baseline	8 mandatory provisions applying to all ICT contracts	Art. 30(2) provisions PLUS enhanced requirements
Key provisions	Service description · Data security · SLAs · Incident cooperation · Termination rights · Training	Full quantitative SLAs · TLPT cooperation · Unrestricted audit rights · Contingency plans · Exit strategy
Audit rights	Not explicitly mandated at Art. 30(2) level	Unrestricted access, inspection & audit — financial entity, appointed third party AND regulator
Exit strategy	Termination rights (Art. 28(7))	Mandatory documented exit plan with transition period

⚠️ CIF classification determines which tier applies — getting this wrong affects every contractual obligation.

Art. 30(2): Mandatory Provisions for All ICT Contracts

- **Written agreement required — full contract including SLAs in one written document**
- **8 minimum provisions applicable to ALL ICT contracts:**
 - ① Complete description of ICT services + permitted subcontracting conditions
 - ② Data location and processing locations (+ notification obligation for any change)
 - ③ Data security: availability · authenticity · integrity · confidentiality
 - ④ Data access, recovery and return in accessible format (on insolvency / termination)
 - ⑤ Service level descriptions (including updates and revisions)
 - ⑥ Incident assistance + cooperation with competent authorities
 - ⑦ Termination rights and minimum notice periods
 - ⑧ ICT security awareness and digital operational resilience training participation

Art. 30(3): Enhanced Provisions for CIF Contracts

- **In addition to Art. 30(2) — the following must also be included in all CIF contracts:**
 - ① Full SLAs with precise quantitative AND qualitative performance targets
 - ② Notice periods + material impact reporting obligations on provider
 - ③ Business contingency plans + ICT security measures — tested by provider
 - ④ Obligation to participate in and cooperate with TLPT
- **⑤ Unrestricted audit & inspection rights:**
 - → By financial entity · appointed third party · AND competent authority
 - → Right to take on-site copies; cannot be limited by other contractual arrangements
 - → Pooled audit alternative available where other clients' rights are affected
 - ⚠ Microenterprise exception: may delegate audit to independent third party
- **⑥ Exit strategies and mandatory adequate transition period**
 - → Continued provision during transition + migration to alternative provider or in-house solution

F.

Exit Strategies & Ongoing Monitoring

Exit Strategies: Art. 28(8) & RTS 2024/1773

- **Required for ALL CIF arrangements**
- **Step 1 — Triggers (Art. 28(7) & (8))**
 - Provider failure or quality deterioration
 - Business disruption due to failed ICT service provision
 - Breach of applicable law, regulations or contractual terms
- **Step 2 — Exit plan requirements (RTS 2024/1773)**
 - Documented · realistic · based on plausible scenarios · periodically tested and reviewed
 - Covers 3 scenarios: unforeseen interruption · failed service delivery · unexpected termination
- **Step 3 — Enable exit without:**
 - ✗ Disruption to business activities
 - ✗ Limitation of regulatory compliance
 - ✗ Detriment to continuity and quality of services to clients
- Include: alternative provider plan or in-house migration + contingency measures

Ongoing Monitoring: RTS 2024/1773



- **Continuous performance monitoring via KPIs and key control indicators**
- **Provider reporting obligations (contractually embedded)**
 - → Periodic reports · Incident reports · Service delivery · Security · Business continuity testing
- **Shortcomings**
 - Document remediation measures with defined timeframes · Monitor implementation
- **Audit rights in practice — strict conditions on certification reliance**
 - ✗ Cannot rely solely on certifications or third-party audit reports over time
 - ✓ Certifications accepted only if: correct scope, not obsolete, right to request scope changes retained
 - ✓ Right to perform individual and pooled audits must be preserved and exercised
- **Periodic re-assessment required when:**
 - Business environment changes · New ICT threats · Geopolitical risks · Concentration risk evolution

G.

Subcontracting Chains & ICT Concentration Risk

Subcontracting CIF Services: Pre-Conditions (RTS 2025/532)



- **Before permitting subcontracting of CIF-supporting services, 4 mandatory pre-conditions must be met:**
 - ① **Provider selection & chain transparency**
 - Provider can select and assess subcontractors and identify the full subcontracting chain
 - Provider must notify the financial entity of all subcontractors supporting CIFs
 - ② **Flow-down of rights**
 - Subcontractors grant financial entity and regulators the same access, inspection and audit rights as the primary provider
 - ③ **Financial entity's own assessment**
 - Financial entity has assessed: subcontractor failure impact · location risks · concentration risk · audit obstacles
 - ④ **Continuous oversight capability**
 - Provider monitors subcontracted services and ensures continuity throughout the chain if a subcontractor fails

Subcontracting: Material Changes & Termination Rights (RTS 2025/532)

- **Material changes to subcontracting → mandatory prior notification to financial entity**
 - Reasonable notice period for the financial entity to approve or object
 - Provider may only implement changes after approval or after notice period expires without objection
 - Financial entity may object and request modifications if changes exceed its risk tolerance
- **Right to terminate the primary contract where:**
 - → Financial entity objected but provider implemented changes regardless
 - → Changes were implemented before the end of the notice period without approval
 - → Provider subcontracts a CIF service not explicitly permitted under the primary contract
- **Periodic re-assessment of subcontracting risks required against:**
 - Changes in supported business functions · ICT threats · Concentration risks · Geopolitical risks

ICT Concentration Risk (Art. 29)

- **1. Entity-level concentration**
 - Multiple CIF arrangements relying on the same or closely connected providers
 - Assessment required at entity, sub-consolidated and consolidated level
- **2. Supply chain concentration**
 - Critical services concentrated at a single subcontractor deep in the chain
- **3. Non-substitutability assessment**
 - Market share · Proprietary technology · Migration cost and complexity
 - Limited number of realistic alternative providers in the market
- **Documented in the register (ITS 2024/2956 — Template B_07.01)**
 - Substitutability score · Date of last audit · Impact of discontinuation
 - ⚠ Periodically re-assessed as new arrangements are added and the business environment changes

H. CTPP Oversight Framework

Critical ICT Third-Party Providers (CTPPs): Designation



- **Designated by ESAs (EBA/ESMA/EIOPA) via Joint Committee on Oversight Forum recommendation**
- **Two-step designation assessment:**
 - **Step 1 — Systemic impact:** total assets of client financial entities; number of G-SIIs/O-SIIs relying on provider; cross-sector CIF reliance
 - **Step 2 — Substitutability:** market alternatives, migration cost and complexity, proprietary technology
- **Lead Overseer**
 - Assigned to EBA, ESMA or EIOPA based on financial entities with the largest share of total assets using that provider
- **Third-country CTPPs**
 - ⚠️ Must establish an EU subsidiary within 12 months of designation
- **Excluded from designation:**
 - Intra-group ICT providers · Providers serving only one Member State

CTPP Oversight: Lead Overseer Powers & Consequences for Financial Entities



- **Lead Overseer powers over CTPPs (Arts. 35–39)**
 - → Request all relevant information and documentation
 - → Conduct general investigations and on-site inspections (including in third countries)
 - → Issue recommendations on ICT security, service conditions, subcontracting plans
- **Enforcement**
 - ⚠ Periodic penalty payments: up to 1% of average daily worldwide turnover, per day, up to 6 months
 - Public disclosure of CTPP non-compliance
- **Consequences for financial entities using a CTPP**
 - → CTPP recommendations must be integrated into ICT third-party risk management
 - → Regulators may require suspension or full termination of use of a non-compliant CTPP
 - → CTPP designation = material risk event triggering review and notification obligations

I. Key Takeaways

Key Takeaways: Building a Bulletproof Third-Party Risk Framework

1. Classify functions first

- CIF classification drives the entire framework — invest in a robust, documented methodology

2. Build the register now

- ITS 2024/2956 templates define exactly what regulators expect — maintain and update continuously

3. Govern actively

- Strategy, officer and CIF policy are management body responsibilities — not legal/compliance alone

4. Negotiate proactively

- Audit rights and exit strategies must be embedded in contracts — very hard to retrofit

5. Map your supply chain

- Know who is at rank 2, 3 and beyond for your CIF arrangements (RTS 2025/532)

6. Monitor and test

- KPIs, audits and tested exit plans are the difference between paper compliance and real resilience

Thank You



Partner

Information Communication

Technology (ICT)

Information Governance & Data

Protection (Privacy)

+32 (0)2 787 90 93

bastiaan.bruyndonckx@lydian.be