A RESIVIA PRODUCT

DORAssure

CONTINUITY WHITEPAPER

Operational Continuity for Critical ICT Systems: The DORAssure Framework

From pre-trigger readiness through to a replatformed, fully operational system — a complete engagement framework for financial institutions facing ICT vendor risk.

THE PROBLEM

The Gap in Existing Continuity Models

Financial institutions depend on increasingly complex, bespoke ICT systems for critical functions — trading, settlement, risk, and client services. When the vendors who built and operate those systems fail, are acquired, or become unresponsive, the institution faces a structural problem: the code may exist somewhere, but the ability to operate it does not.

Legacy continuity models fall into two inadequate categories. Source code escrow protects intellectual property but provides no operational capability. Business continuity planning documents intent but provides no tested activation pathway.

DORA, PS21/3, and ESMA's guidelines now require **demonstrable** operational continuity — not documented intent. The gap between documentation and demonstration is where most firms are exposed.

> "[Firms should] develop exit plans that are comprehensive, documented and sufficiently tested."
>
> — ESMA, GUIDELINES ON OUTSOURCING TO CLOUD SERVICE PROVIDERS (GUIDELINE 5: EXIT STRATEGIES)

FRAMEWORK OVERVIEW

Five phases from pre-trigger to full operation

01	02	03	04	05
Gather	Trigger	Step-In	Replatform	Operate

THE FIVE-PHASE DORASSURE FRAMEWORK

01

GATHER — PRE-TRIGGER KNOWLEDGE CAPTURE

DORAssure works directly with the client and, where accessible, with the incumbent vendor to capture complete operational knowledge. This includes system architecture documentation, build and deployment procedures, operational runbooks, configuration management, and escalation paths. Where the vendor is unavailable or uncooperative, we work from client-side knowledge and system observation.

> **Deliverables:** Architecture map, full system requirements specification, runbook library, deployment guide, configuration baseline. Updated quarterly and on material system changes.

02

TRIGGER — ACTIVATION

Activation may be triggered by a range of events: vendor insolvency, material service failure, regulatory direction, client election to exit, or contractual breach. Trigger conditions are pre-agreed and documented in the DORAssure engagement agreement — avoiding any ambiguity about when activation rights apply.

Activation is the client's election — DORAssure does not independently trigger. Once triggered, the clock starts on the 48-hour step-in SLA.

03

STEP-IN — 48-HOUR OPERATIONAL TAKEOVER

Within 48 hours of activation, DORAssure engineering assumes operational control of the critical systems. This includes deploying from the active build environment, assuming monitoring and alerting responsibilities, managing the incumbent vendor handover (where applicable), and establishing direct communication with the client's operational teams.

The 48-hour SLA is contractually committed and backed by on-call engineering. It is not a best-efforts timeline — it is a performance obligation. Step-in does not require vendor cooperation to succeed.

04

REPLATFORM — MODERN ARCHITECTURE REBUILD

While the stabilised system operates under step-in, DORAssure begins the replatforming engagement. This is the defining difference between DORAssure and legacy continuity models: we do not simply keep the lights on indefinitely on legacy infrastructure. We rebuild.

Replatforming delivers: modern architecture aligned with current engineering standards, clean intellectual property documentation, regulatory-grade audit trails, comprehensive codebase documentation, and a system the client owns outright — whether they choose to operate it themselves or engage DORAssure to do so.

Replatforming scope and timeline are pre-agreed at engagement signing. Fees are fixed based on our initial assessment and agreed upfront — no surprises at the time of activation.

05

OPERATE — SAAS OR BUILD & TRAIN

Once replatforming is complete, the client chooses their operating model — agreed at contract signing, not under pressure post-activation.

SaaS Model: DORAssure operates the replatformed system as a managed service. We own the IP, provide SLA-backed uptime, handle all infrastructure and evolution. The client receives a fully operational, continuously maintained platform without internal engineering overhead.

Build & Train: DORAssure transfers full IP ownership to the client. We train the client's internal team over a structured 6–12 month programme, provide comprehensive documentation, and support the transition to full internal operation. At handover, the client owns a modern, well-documented codebase they control entirely.

HOW WE WORK

Commercial Structure

DORAssure engagements are structured around a single, transparent commercial framework with no ambiguity about what activates when.

Setup fee — At engagement signing

Covers initial knowledge capture, architecture mapping, build environment setup, and first quarterly exercise. Sized to engagement scope.

Annual retainer — Optional

Covers ongoing codebase sync, documentation upkeep, environment hosting, and quarterly readiness exercises. Required for firms with quarterly testing obligations under DORA or PS21/3.

Activation + Replatforming fee — Pre-agreed, activated on trigger

Fixed at contract signing based on our initial assessment and agreed upfront — no surprises at the time of activation. Covers step-in, stabilisation, and full replatforming. Structured in two tranches: step-in (on trigger) and replatform completion (on delivery).

Operate & Transition fee — Pre-agreed, model chosen at signing

SaaS model: ongoing managed service fee. Build & Train: structured programme fee over the transition period. Both pre-agreed — no renegotiation under pressure.

THE STRATEGIC CASE

Why Replatforming, Not Just Continuity

The instinct in operational continuity is to preserve the status quo — keep the legacy system running until a long-term decision can be made. Resivia's position is that this instinct is strategically wrong and increasingly unaffordable.

Legacy systems that survive vendor failure events typically do so on outdated infrastructure, with undocumented codebase, unclear IP, and no path to evolution. The temporary holding pattern becomes permanent, and the firm finds itself operating a system no one fully understands at increasing maintenance cost with no regulatory audit trail.

Replatforming at the point of transition — when change is already occurring — is structurally cheaper, faster, and lower-risk than retrofitting it later. DORAssure's model treats every activation as an opportunity to arrive on the other side of the disruption with a better system, not just the same one under new management.

Ready to talk through the framework?

Request a readiness assessment — we'll review your current continuity position and identify any gaps against your regulatory obligations.

Request a Readiness Assessment →

FOR REGULATED FIRMS

Demonstrate operational continuity to your regulator with a tested, contractually-backed activation pathway. Not documented intent — demonstrated capability.

FOR TECHNOLOGY VENDORS

Offer your financial-sector clients a drop-in continuity operator. Turn the DORA Article 28 exit question from a procurement objection into a selling point.