Luxgap
DATA PRIVACY PARTNER

REGULATION (EU) 2022/2554

IN EFFECT SINCE JANUARY 17, 2025

DORA — Digital Operational Resilience Act

Transition from "paper" compliance to a **measurable operational resilience**. Luxgap supports your teams in reducing ICT risk, meeting supervisory requirements, and industrializing the management of incidents, tests, and third-party providers.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116

Why DORA is truly a game-changer

The DORA (Digital Operational Resilience Act) regulation marks a major turning point in the regulation of the European financial sector. For the first time, a text imposes **uniform and binding requirements** on the security of networks and information systems supporting the business processes of all financial entities — and their ICT third-party service providers.

Unlike previous directives, DORA is not limited to recommendations: it demands **tangible proof** of effective operational resilience. "Declarative" compliance is no longer sufficient. Supervisors now expect *provable* resilience, based on artifacts, operated processes, and documented traces.

ICT Risk Management

Comprehensive framework, policies, inventories, controls, BCP/DR, and continuous monitoring of technological risks

Incident Reporting

Major ICT incidents + voluntary notification of significant cyber threats using harmonized EU templates

Resilience Testing

Risk-adapted testing program including TLPT for significant entities

Information Sharing

Controlled mechanisms for sharing intelligence on cyber threats and vulnerabilities between entities

ICT Third-Party Risk

Supervisory framework for critical third-party providers, register, contractual clauses, and exit strategies

➡️ **DORA Objective**: *evidence-based* resilience — each requirement must be supported by concrete evidence, not mere statements of intent.

Who is concerned? Scope in practice

DORA targets **almost the entire European financial ecosystem**. Its scope is intentionally broad: it is no longer about regulating only large banks, but about ensuring the resilience of the entire financial value chain, including the actors that technologically depend on it.

Financial entities directly subject

- **Credit institutions** (commercial banks, investment banks)
- **Insurance and reinsurance undertakings**
- **Investment firms** and asset management companies
- **Market infrastructures** (CCPs, central securities depositories, trading venues)
- **Payment institutions** and electronic money institutions
- **Insurance intermediaries** — including ancillary (explicit reference to Art. 2(1) of the regulation)
- **Occupational pension funds**, credit rating agencies, benchmark administrators
- **Crypto-asset service providers**

ICT service providers — indirectly but heavily impacted

Even without being directly regulated, your ICT providers are concerned **by ripple effect** via the obligations DORA imposes on financial entities:

- **Cloud providers** (IaaS, PaaS, SaaS)
- **SOC / MSSP** (Security Operations Centers)
- **Critical SaaS vendors**
- **MSP / IT service managers**
- **Data providers** and hosting providers

Implications: strengthened contractual obligations, information register, right of audit, data localization requirements, and documented exit strategy.

OVERVIEW

The 5 DORA Pillars — and the Expected "Proof"

DORA is structured around five fundamental pillars. Each one is not limited to a documented policy: supervisors expect **concrete artifacts**, **continuously operated processes**, and **verifiable traces** (logs, tickets, test reports, committee decisions, crisis communications).

➡️ **Each pillar = artifacts + operated processes + traces.** European supervision rewards consistency, traceability, and execution capability — not the volume of documentation.

Our Luxgap Promise: Useful DORA = Resilience + Control

At Luxgap, we believe that DORA compliance is only valuable if it truly **serves your operational resilience**. We don't deliver binders – we build measurable, tested, and auditable capabilities. Our approach transforms every regulatory requirement into a concrete lever for risk reduction and operational performance improvement.

1

Reduce Downtime

Proactive prevention, rapid detection, structured response, and accelerated restoration. Every minute of preserved availability protects your revenue and customer trust.

2

Accelerate Crisis Decision-Making

Clear roles, pre-established scenarios, operational runbooks, and ready-to-use communication plans. In a crisis, decision speed is your primary shield.

3

Secure ICT Outsourcing

Compliant contracts, updated information register, effective audit rights, and tested exit strategy. Your service providers become resilience partners, not sources of risk.

4

Succeed in Controls

Structured "audit-ready" file, consistent evidence, group traceability. You approach each inspection with confidence and demonstrate your mastery.

5

Industrialize the Approach

Continuous measurement, regular testing, iterative improvement, and team training. Compliance is not a one-time project – it's an ongoing discipline.

PILLAR 1

ICT Risk Management — What DORA concretely requires

DORA's first pillar forms the foundation of the entire framework. It mandates an ICT risk management framework described as **« sound, comprehensive and well-documented »**. This is not a theoretical exercise: supervisors expect a living framework, operated daily, with each component supported by concrete evidence. Luxgap implements — or strengthens — every building block of this framework.

ICT Governance

Clear definition of roles and responsibilities, creation or strengthening of dedicated committees (ICT risk committee, security committee), implementation of reporting to the management body. Article 5 of DORA makes the management body **directly responsible** for the ICT risk management framework.

ICT Inventory & Classification

Exhaustive mapping of ICT assets (systems, applications, data, networks), classification of services and functions as **« critical / important »**, identification of internal and external dependencies — including the subcontracting chain.

Policies & Standards

Drafting or updating policies covering: access management (IAM), encryption, vulnerability management, logging, change management, network security. Each policy is aligned with EBA's RTS.

BCP/DR — Continuity & Recovery

Business continuity and disaster recovery plans covering critical functions, defined restoration objectives (RTO/RPO), documented regular tests, and iterative updates after each exercise or actual incident.

Monitoring & Indicators

Implementation of key risk indicators (KRIs), early warnings, and dashboards to track control effectiveness. Monitoring must be **continuous**, not ad-hoc — DORA requires active surveillance of threats and vulnerabilities.

Sources: Art. 6 of DORA regulation (ICT framework); RTS ICT risk management framework (EBA)

PILLAR 1 — DEEP DIVE

The « DORA Evidence Pack » — Your Key to Audit Success

One of the most significant changes introduced by DORA is the requirement for **tangible and traceable evidence** for each component of the ICT framework. Supervisors no longer merely read policies: they verify their effective application. Luxgap builds for you a structured, maintainable, and directly usable **DORA Evidence Pack** for audits.

01

Asset Register & Mapping

Exhaustive inventory with "critical / important" classification for each asset, service, and function. Mapping of interdependencies and identification of Single Points of Failure (SPOF).

ĆČ

Controls Catalog

Three-dimensional mapping: DORA requirements ↔ controls ↔ evidence. Each regulatory requirement is linked to one or more operational controls, themselves supported by verifiable evidence.

03

Business Continuity / Recovery Policy

Complete BCP/DR documentation including test results, identified deviations, corrective actions taken, and management validations.

ĆÇ

KRI Dashboards

Key Risk Indicators covering: open vulnerabilities, ongoing incidents, availability of critical systems, control compliance. Historical monitoring and trends.

05

Prioritized Remediation Plan

Prioritization by risk criticality, implementation effort, and dependencies. Milestone tracking, identified owners, and progress reporting to management.

Luxgap Tip: A well-structured evidence dossier reduces preparation time for audits by 40-60% and eliminates the stress of last-minute inspections.

PILLAR 2

Testing & TLPT — Moving Beyond the "Annual Pentest"

DORA significantly raises the bar for resilience testing requirements. Gone are the days of annual "checkbox" penetration tests: the regulation mandates a testing program tailored to each entity's risk profile, covering the entire spectrum — from vulnerability scans to crisis exercises and recovery tests. For the most significant entities, DORA may impose Threat-Led Penetration Testing (TLPT), aligned with the TIBER-EU framework.

Testing Strategy

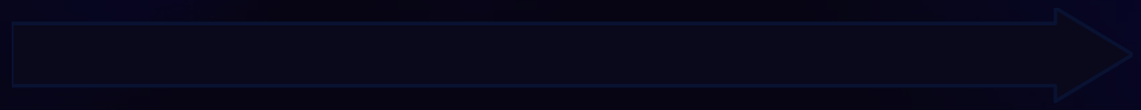
Design of a multi-year program integrating: vulnerability scans (weekly), configuration reviews, penetration tests (pentests), crisis management exercises, business continuity and recovery tests (DR tests). Each test type is calibrated to the criticality of the functions involved.

Testing Governance

Definition of tester independence, scope covered, result acceptance criteria, and retest conditions. Governance ensures that tests produce actionable and unbiased results.

Remediation Chain

Systematic tracking of identified vulnerabilities, remediation SLAs by criticality, validation of corrections, and automated retesting. No flaw goes untracked.



TLPT Preparation

For eligible entities: TIBER-EU aligned approach, preparation of the supervisory file, selection of threat intelligence and red team providers, management of specific RTS requirements for TLPT.

Sources: art. 24-27 of the DORA regulation; RTS TLPT (TIBER-EU reference)

⚠ PILLAR 3

Incident Management & Reporting — Harmonized Classification and Notification

DORA significantly standardizes the classification of ICT incidents and notification deadlines to competent authorities at the European level. The RTS and ITS published in 2024-2025 precisely define the criteria, thresholds, templates, and schedules. The reaction window is tight: **4 hours after classification** for initial notification, 72 hours for the interim report, and 1 month for the final report.

Regulatory Deadlines

1 **Detection → Classification**

Incident identification and application of "major / non-major" classification criteria according to RTS 2024/1772

2 **Initial Notification: 4h**

After classification (and within 24 hours of detection). Transmission to competent authorities via harmonized ITS 2025/302 templates

3 **Interim Report: 72h**

Update of analysis, measures taken, impact estimation, and initial corrective actions initiated

4 **Final Report: 1 month**

Complete incident analysis, root causes, definitive impact, lessons learned, and corrective actions

The Luxgap Incident Reporting Kit

We deliver a complete operational kit, directly usable by your SOC, IT, legal, and communication teams:

Decision Tree

"Major / non-major" criteria and thresholds formalized, classification RACI, automatic escalation to the right stakeholders

Operational Playbooks

SOC, IT, Legal, and Communications procedures — covering internal notification, to authorities, and to impacted clients

Pre-filled Templates

EU harmonized forms pre-completed with your entity's static data + collection procedure ensuring quality and traceability

PILLAR 3 — OPERATIONAL MODEL

Our "7-Phase" Model — From Obligation to Actionable Incident Process

Luxgap does not simply document an incident procedure: we transform the DORA obligation into an **operational process ready to execute**, regularly tested and backed by evidence at each step. This model covers the entire incident lifecycle, from preparation to continuous improvement.

1. Preparation & Prevention

Risk scenarios, threat intelligence, hardening, team training, pre-positioning of tools and contacts

2. Detection & Immediate Response

Automated alerts, initial triage, RACI activation, initial notification within regulatory deadlines

3. Containment, Eradication & Mitigation

Isolation of affected systems, threat elimination, reduction of impact on critical functions

4. Recovery & Restoration

Restoration of services according to RTO/RPO objectives, data integrity verification, gradual resumption of operations

5. Post-Incident Analysis & Adaptation

Root cause analysis, documented timeline, lessons learned, final report to authorities, control adjustments

6. Continuous Improvement & Update

Integration of feedback, procedure updates, alert recalibration, scenario enrichment

➡️ **The differentiating factor:** at each phase, **evidence** is generated and retained — tickets, timestamped timelines, committee decisions, traced communications. This discipline of traceability makes all the difference in auditing.

PILLAR 4

ICT Third-Party Risk — The Real Challenge: Register, Contracts & Exit

DORA's Pillar 4 often generates the most operational work. It's no longer just about "managing suppliers": DORA demands **complete mastery of the ICT outsourcing chain**, with precise contractual obligations, a standardized information register, and genuinely testable exit strategies. Level 2 texts (RTS and ITS) published in 2024-2025 detail each requirement.

RTS 2024/1773

Policy on contractual arrangements for ICT services supporting critical or important functions

ITS 2024/2956

Standardized information register on ICT arrangements — format, content, and update frequency

RTS 2025/532

Specific requirements on ICT outsourcing, including the sub-contractor chain

What Luxgap operates for you

1

Complete Inventory

Mapping of all ICT providers, criticality assessment, identification of dependencies — including the often-overlooked "chain of subcontractors." Concentration risk analysis.

2

Contractual Remediation

Review and compliance of clauses: right to audit, data access, localization, incident notification, performance and security SLAs, transferability, cooperation with authorities.

3

Testable Exit Strategy

Documented exit plan for each critical provider: data reversibility, service continuity during transition, identified alternatives, and periodic testing of plan feasibility.

REGULATORY FOCUS

Oversight of Critical Third-Party Providers (CTPP) — Anticipating Controls

The European Supervisory Authorities (ESAs: EBA, EIOPA, ESMA) have the power to **designate ICT providers as "critical" (CTPP — Critical Third-Party Providers)**, subjecting them to a direct supervision framework. This designation has major implications — not only for the provider, but for **all financial entities that depend on them**.

Implications for your organization

Even if you are not a cloud provider, your contracts and governance must meet strict requirements:

Auditability & Access

Your contracts must ensure that supervisory authorities — and you yourself — can audit the provider, access its premises, and obtain necessary information. This right cannot be limited by confidentiality clauses.

Concentration & Dependencies

You must identify and control concentration risks: how many critical functions depend on the same provider? Are viable alternatives available? Is the systemic risk documented?

Credible Exit Strategy

The exit strategy cannot be a theoretical document filed away. It must be **realistic, tested, and updated** — with migration timelines, estimated costs, and operational alternatives.

What Supervisors Reward: Consistency + Traceability

Feedback from initial inspections clearly shows what distinguishes a "robust" DORA program from a fragile one. Supervisors are not looking for perfection: they are looking for **consistency**, **traceability**, and **execution capability**. Here are the concrete markers that make a difference during an audit.

A Living ICT Register

Ready to be submitted to authorities at any time, with a **documented update process** and identified responsible parties. Not an Excel file frozen for 6 months — an operational register continuously updated.

Incidents Classified Reproducibly

Classification criteria applied homogeneously, formalized decision tree, and **timely reporting** — 4h, 72h, 1 month. The reproducibility of classification is a key audit point.

Tests Planned, Monitored, and Retested

Documented testing program, tracked results, **remediation managed with SLA**, and systematic retesting of corrected vulnerabilities. End-to-end monitoring is proof of a mature approach.

DORA-Aligned Contracts

For all critical and important functions: RTS-compliant clauses, effective audit rights, incident notification, documented SLAs, and **credible exit strategy**.

LUXGAP OFFERING

À la carte Modules — Guaranteed Results, Backed by Evidence

Our DORA offering is designed to adapt to your maturity level and priorities. Each module is autonomous and can be activated independently, while integrating perfectly into a global approach. From initial diagnosis to continuous operation, we cover the entire lifecycle of your DORA program.

1. DORA QuickScan

Management + IT + Risk + Legal

Applicability mapping, scope definition, current maturity level assessment, and priority identification. Deliverable: positioning report with immediate action recommendations.

2. DORA Gap & Roadmap

Pillar by pillar

Detailed gap analysis against DORA and RTS/ITS requirements, target definition, construction of a prioritized remediation plan with effort estimation, dependencies, and implementation schedule.

3. DORA Build

Implementation & Documentation

Operational construction: drafting of policies and procedures, implementation of the information register, creation of the incident kit, design of the testing program, development of compliant vendor clauses.

4. DORA Run

Operation & Continuous Improvement

Operational management of the program: monitoring dashboards, regular exercises, periodic reviews, continuous updating of evidence and documentation. Compliance becomes an enduring discipline.

💡 **"Continuous Improvement" Logic:** Each module feeds the next. Evidence generated in the Build phase is maintained in the Run phase. Feedback from exercises enriches identified gaps. Your DORA program gains maturity with each cycle.

Tangible Deliverables — What you can show tomorrow during an audit

Each Luxgap deliverable is designed to be directly usable in an audit or control situation. No abstract documentation: only **operational, structured, and maintainable artifacts** that demonstrate your mastery of each DORA pillar.

ICT Risk Management Framework

Complete framework including requirements ↔ controls ↔ evidence mapping. A living document serving as a reference for the entire program.

Inventory of Critical Assets & Functions

Register of ICT assets, services, and functions with criticality, internal/external dependencies, and associated risk mapping.

Testing Program

Multi-year planning, test scenarios, execution reports, remediation tracking, and retests. Formalized governance and acceptance criteria.

Incident Reporting Kit

Classification tree, RACI, notification templates (ITS), data collection procedure, and playbooks by stakeholder type.

Provider Register (ITS)

Information register compliant with ITS 2024/2956 format, documented maintenance process, and alerts on contractual deadlines.

Contractual Policy & Exit Plan

Compliant clause templates for critical/important functions, testable exit plans per provider, and concentration risk analysis.

CONTINUOUS SERVICE

DORA-as-a-Service — What makes the offering useful daily

DORA compliance doesn't stop at "Go Live". Requirements are continuous, threats evolve, and supervisors expect **permanent improvement**. Luxgap offers recurring support that keeps your DORA program alive, operational, and up-to-date — without constantly mobilizing your teams.

E-learning & Awareness

Continuous and traceable training program covering ICT security and operational resilience. Modules adapted by profile (management, IT, business, compliance). Each session is documented to provide proof of training during controls — in accordance with DORA's requirement for employee awareness.

Weekly Vulnerability Scans

Automated scans across the entire ICT perimeter, with vulnerability reports categorized by criticality. Integrated remediation tracking: each vulnerability is tracked until resolution. Full history available to demonstrate correction discipline.

Document Review & Update

Periodic review of the entire documentary corpus: policies, standards, procedures, evidence. Proactive updating based on regulatory changes (new RTS/ITS, ESAs guidelines) and internal feedback.

Periodic Reviews

Regular exercises (incident tests, DR, crisis), review of continuity plans, analysis of incidents that occurred, and integration of lessons learned into the program. Each review produces a documented report feeding into the DORA Evidence Pack.

Why Luxgap — Our Differentiation

The regulatory compliance consulting market is not short of players. What distinguishes Luxgap is our ability to articulate **legal requirements and operational reality** — to produce compliance that works in practice, not just on paper.

Dual perspective: legal + technical

We master both regulatory obligations (DORA regulation, RTS, ITS, ESAs guidelines) and their operational translation (controls, runbooks, technical evidence). This dual expertise avoids the frequent disconnect between what the text requires and what IT teams implement.

Supervision-oriented approach

We know what supervisors look for during an inspection: **consistency between documentation and reality**, traceability of decisions, and demonstrated execution capability. Our approach is calibrated to maximize your audit performance.

Pragmatic approach

We prioritize real risks and critical functions, without unnecessary "paperware". Every deliverable has an identified operational use. We refuse documentation that exists only for its own sake.

Sustainable industrialization

Continuous team training, automated scans, recurring document maintenance — we implement mechanisms that keep your compliance alive over time, without excessive dependence on external consulting.

> “What matters in control = consistency, traceability, execution. Luxgap builds DORA programs that stand the test of reality — not just paper.”

TAKE ACTION

Next Step — Simple and Effective

DORA has been in effect since **January 17, 2025**. Every day that passes without a structured program increases your regulatory and operational exposure. The good news: there is still time to build a robust framework, provided you act now with a clear method.

1

Scope Definition

Identification of concerned entities, critical and important functions, and ICT third-party service providers. Definition of the program boundaries and key stakeholders.

2

QuickScan & Prioritization

Rapid assessment of your DORA maturity, identification of major gaps, and prioritization by risk criticality, business impact, and implementation effort.

3

Launch of "Must-Haves"

Immediate start on the fundamentals: information register, incident kit, contractual remediation, testing program, and evidence collection.

01/17

Effective Date

DORA has been fully applicable since January 2025

5

Pillars of Requirements

Covering risks, testing, incidents, third-party providers, and information sharing

4h

Notification Deadline

For major ICT incidents after classification

Contact Luxgap today to schedule your QuickScan and embark on your journey towards measurable, demonstrable, and sustainable operational resilience.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116