
DORA and the new architecture of operational resilience

Control, continuity, and technology choice.

aruba.it

RESILIENCE

The Digital Operational Resilience Act (DORA) represents a cornerstone of the European Union's strategy to strengthen the stability of the financial system in the digital age. Regulation (EU) 2022/2554 establishes a harmonized framework for ICT risk management, designed to prevent, withstand, respond to, and recover from technology-related incidents that could undermine market stability and financial continuity.

Within the evolving European regulatory framework, data integrity, cybersecurity, and digital trust are no longer secondary features of IT infrastructure; they are structural components of the operational architecture of financial institutions. Compliance must therefore be embedded at the design stage rather than applied retrospectively as an add-on. This shift transforms regulatory alignment into a strategic lever, enabling organizations to evolve toward more resilient, adaptive, and secure operating models.

The level of operational resilience required by DORA calls for a **compliance-by-design** approach, where regulatory requirements are integrated into architectural and operational decisions from the outset. In practice, this leads to an end-to-end integrity model, in which trust, security, and traceability are embedded across the entire digital stack, from physical data center infrastructure to cloud environments, network layers, applications, and the most distributed digital interactions.

This paper examines the key operational pillars of DORA and outlines practical guidelines to help banks, insurance companies, and financial market infrastructures (FMIs) build measurable digital resilience, not merely declared compliance.

Many organizations describe themselves as “resilient,” yet only a limited number can demonstrate this capability under operational stress or regulatory scrutiny. Achieving real resilience requires concrete technology decisions, integrated governance models, and consistent execution across the entire organization.

Recent disruptions affecting global hyperscalers illustrate this challenge: large-scale outages have temporarily halted entire digital ecosystems, generating cascading effects across financial services and critical infrastructures.

DORA introduces a fundamental shift in perspective. Digital infrastructure is no longer a purely technical domain, it is a central component of financial stability, directly linked to IT risk management, cybersecurity resilience, and service continuity.

Over the past decade, the financial sector has widely adopted cloud computing and global technology providers, gaining significant advantages in scalability, performance, and innovation capacity. At the same time, this evolution has introduced systemic exposure. Dependence on a limited number of large vendors can create concentration risks. DORA addresses this structural vulnerability by reinforcing the ICT operational resilience framework:

- **integration into a harmonized EU regulatory framework;**
- **direct accountability of board-level governance;**
- **extended oversight across the entire digital supply chain.**

Formal compliance, based on policies, documentation, and procedural checklists, is no longer sufficient. Operational resilience emerges from a structured and continuous effort that aligns people, processes, technologies, and governance well before any incident occurs.

The central question becomes clear: **can the organization ensure operational continuity, technological control, and verifiable digital resilience?**

DORA reframes this challenge by moving it beyond a purely technical scope and placing it within the broader context of governance, digital sovereignty, and financial system stability.

Operational resilience is not limited to incident management or regulatory compliance. Increasingly, it requires organizations to maintain long-term control over their technology choices and infrastructure evolution.

Digital risk management, vendor concentration risk, and architectural decisions are closely connected to a broader capability: **preserving strategic control, the ability to evolve the technology ecosystem without losing governance over data, infrastructure, and future strategic options.**

Summary

01 Foundations and pillars of operational resilience	5
02 Who DORA applies to	7
03 Regulatory timeline and implementation milestones	8
04 The role of people and skills	9
05 Practical toolkit: contractual and operational requirements	10
06 ICT vendor management and monitoring	12
07 Extending digital risk management: the role of brand protection	13
08 Concentration risk: an often underestimated systemic factor	15
09 Aruba and operational resilience in the context of DORA	17
10 The new currency of financial trust	19
11 Conclusions and priority actions	21

CHAPTER 01

Foundations and pillars of operational resilience

DORA establishes a harmonized regulatory framework for ICT risk management that applies to thousands of European financial entities and their information and communication technology (ICT) providers.

The objective is to overcome the fragmentation of national regulations and establish a common European approach to digital operational resilience. This involves strengthening cybersecurity measures while, in a broader perspective, building a risk management model capable of preventing disruptions, managing incidents, and rapidly restoring critical operational functions, even under severe stress or major disruptions.

1 ICT RISK MANAGEMENT

Financial institutions are required to implement a structured ICT risk management framework under the ultimate responsibility of the management body and executive leadership. This framework must include the identification of critical assets, the definition of resilience strategies, and continuous monitoring processes covering the entire digital infrastructure.

3 RESILIENCE TESTING

DORA introduces mandatory and periodic operational resilience testing programs to verify the ability of financial institutions to withstand severe operational stress scenarios. For systemically relevant financial entities, the regulation requires Threat-Led Penetration Testing (TLPT) every three years, conducted in accordance with the European TIBER-EU framework.

2 INCIDENT REPORTING

ICT-related incidents must be managed through structured classification and reporting procedures based on their impact, severity, and the criticality of the affected services.

Major incidents must be reported promptly to supervisory authorities according to harmonized EU criteria.

4 THIRD-PARTY RISK MANAGEMENT (TPRM)

Operational resilience now extends well beyond internal systems to encompass the entire digital supply chain. DORA requires financial institutions to adopt a structured approach to third-party ICT risk management. The regulation introduces enhanced monitoring mechanisms, specific contractual requirements, and stronger supervisory powers over critical technology providers and infrastructure components.

The DORA framework is built on several core pillars that define the architecture of operational resilience in the European financial ecosystem.

CHAPTER 02

Who DORA applies to

DORA applies to a broad range of entities across the European financial system, as well as to the technology providers that support their operational activities. The regulation functions as a *lex specialis* in relation to the NIS2 Directive: in areas covered by DORA, financial entities follow the regulatory framework defined by the regulation, thereby avoiding overlapping or conflicting compliance requirements.

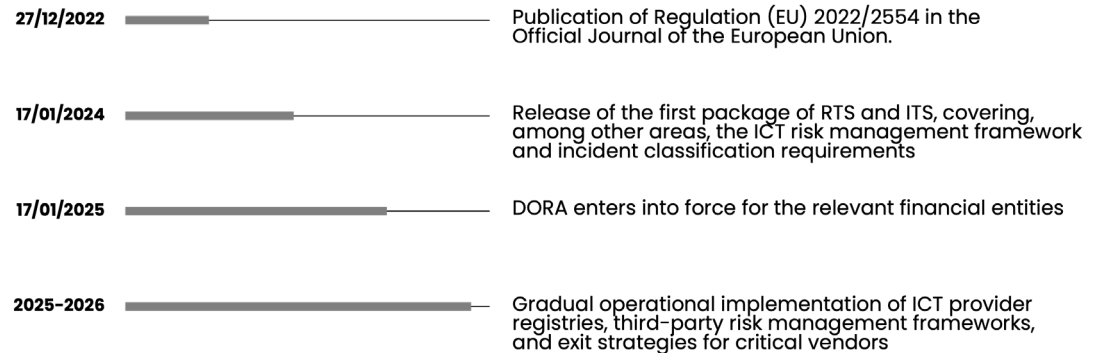
The goal is to establish a consistent and comprehensive operational resilience framework across the entire financial ecosystem, encompassing both regulated institutions and ICT providers that support critical or important functions.

CATEGORY	COVERED ENTITIES	SPECIFIC REQUIREMENTS
FINANCIAL ENTITIES	Banks, insurance companies, electronic money institutions, crowdfunding platforms, crypto-asset service providers (CASPs)	Full or simplified implementation of the DORA framework, with direct accountability of the Board for ICT operational resilience
ICT PROVIDERS	Cloud service providers, data center operators, trust service providers, software vendors	Potential designation as critical ICT providers, subject to direct supervision by European Supervisory Authorities

CHAPTER 03

Regulatory timeline and implementation milestones

Compliance with DORA requires a phased approach, considering not only the text of the Regulation but also the Regulatory and Implementing Technical Standards (RTS and ITS) developed by the European Supervisory Authorities.





CHAPTER 04

The role of people and skills

Digital resilience is often interpreted purely as a technological challenge, yet it is equally dependent on people and organizational capabilities, which must be developed along three key dimensions.

- **Resilience-oriented mindset and organizational culture:** clearly defining roles, responsibilities, and procedures is essential, but equally important is training the organization to act with awareness, speed, and confidence during unexpected events.
- **Awareness at all organizational levels:** every employee, not only IT specialists or cybersecurity personnel, is an integral part of the security ecosystem.
- **Specialized skills for leveraging technology:** beyond technical expertise, employees must possess competencies in governance, risk management, communication, and incident.

For CIOs and CISOs, developing an integrated program of technology adoption and skill development is critical to foster a robust security culture.

Under DORA, continuous training across all levels of the organization is not optional.

Responsibilities and consequences of non-compliance

Compliance with DORA cannot be treated solely as a matter of regulatory, technical, or contractual adherence; it is a governance imperative.

The regulation explicitly assigns ultimate accountability to the management body for ICT risk management and the organization's operational resilience.

Consequently, compliance cannot be delegated entirely to technical or cybersecurity teams. Instead, it must be embedded in strategic governance and supervisory processes.

CHAPTER 05

Practical toolkit: contractual and operational requirements

Effective ICT vendor management under DORA must be grounded in a risk-based mapping aligned with the regulation's framework. This process begins by identifying the business functions supported by critical services, with particular attention to essential or important functions versus other operational activities. For services underpinning these functions, contracts with ICT providers must include specific clauses to ensure transparency, controllability, and operational resilience.

Contracts supporting essential or important functions should incorporate, at a minimum, the following elements.

1

AUDIT AND INSPECTION RIGHTS

Clauses granting the financial entity and competent authorities the right to access information and perform audits, enabling verification of compliance with operational resilience requirements.

2

EXIT STRATEGIES

Defined plans for service and data migration to alternative providers or internal solutions without disrupting critical functions, ensuring continuity during transitions.

3

INCIDENT NOTIFICATION

Contractual obligations for timely reporting of relevant ICT incidents in alignment with DORA's incident reporting standards.

4

SUPPORT FOR ACTIVITIES

Vendor commitment to participate in operational resilience testing, including Threat-Led Penetration Testing (TLPT) where mandated by supervisory authorities.

5

DATA TRANSPARENCY

Clear disclosure of data storage locations, applicable legal frameworks, and security measures implemented to safeguard information.

6

SERVICE LEVEL AGREEMENTS

Definition of service levels and continuity parameters, such as RTO and RPO, consistent with the resilience requirements of the supported functions.

7

SUB-OUTSOURCING MANAGEMENT

Contracts with ICT providers should establish clear conditions for the use of sub-providers, including obligations for notification, transparency.

8

EMERGENCY AND SECURITY PLANS

Vendors must be contractually required to implement, test, and maintain emergency operational plans and adequate cybersecurity measures.

CHAPTER 06

ICT vendor management and monitoring

DORA requires that financial entities maintain an up-to-date registry of ICT vendor agreements supporting operational activities.

This registry serves as a central tool for third-party risk management and monitoring dependence on external technology services.

The registry should enable organizations to clearly identify:

- ICT service providers involved in delivering services;
- business functions supported by these services;
- classification of functions as essential or important;
- vendor risk profiles and concentration levels;
- data portability conditions and exit strategies.

Such information allows financial institutions and supervisory authorities to evaluate supplier concentration, reliance on external infrastructure, and the organization's ability to maintain operational continuity in the event of service disruption.

Operational resilience roadmap

DORA-mandated testing activities should follow a progressive maturity path, designed to strengthen the organization's ability to prevent, detect, and respond to ICT incidents.

Typical Operational Resilience Pathway:

- **Vulnerability Assessment**, identifying technical weaknesses across ICT systems and infrastructure;
- **Gap Analysis**, evaluating the organization's current state against DORA's operational resilience requirements;
- **End-to-End Scenario Testing**, simulating operational stress conditions to verify the continuity of critical business functions.

For systemically important financial entities, **Threat-Led Penetration Testing (TLPT)** is planned in collaboration with supervisory authorities. These advanced tests simulate real-world threat scenarios on a periodic basis.

CHAPTER 07

Extending digital risk management: the role of brand protection



Beyond internal ICT risk management and oversight of the technology supply chain, organizations face an often-underestimated exposure linked to their external digital ecosystem, including brand, service, and institutional identity.

Threat vectors such as phishing, typosquatting, or fraudulent applications that impersonate brands via domain abuse can compromise operational continuity, user trust, and the integrity of digital services, even though these attacks originate outside traditional ICT infrastructure.

In this context, **proactive brand protection complements ICT and Third-Party Risk Management frameworks**. While DORA does not explicitly mandate brand protection, it becomes an integral component of an end-to-end integrity model, enabling organizations to intercept threats that could escalate into material operational incidents.

Integrating brand protection tools into digital risk management processes allows institutions to **strengthen their overall security posture** proactively, **enhance incident detection** and response capabilities, **reduce exposure to external events** that, while not arising from internal vulnerabilities, can significantly affect customers, operations, and regulatory compliance.

CHAPTER 08

Concentration risk: an often underestimated systemic factor

Discussions with financial institutions reveal that technology concentration risk is still frequently underestimated. It is often perceived as a purely technical or infrastructure issue, yet it is fundamentally a strategic operational resilience concern.

European Supervisory Authorities increasingly focus not only on individual ICT incidents but on the level of concentration in technology infrastructure across the financial sector.

When a large number of institutions rely on the same platforms or ICT providers, a systemic vulnerability emerges, with the potential to impact multiple organizations simultaneously.

In such a scenario:

- the likelihood of simultaneous impacts across multiple financial operators increases;
- supervisory and oversight complexity rises;
- the practical ability to migrate to alternative providers diminishes;
- exposure to operational, infrastructure, and geopolitical risks grows.

Technology concentration is no longer a peripheral governance issue; ignoring it introduces an unacceptably high risk to operational continuity and systemic stability.

To address this, DORA introduces a mechanism for identifying critical ICT providers, granting European Supervisory Authorities the mandate to monitor vendors whose operations may have material effects on the financial system.

For boards and executive leadership, this raises a strategic question:

How Distributed Is Our Digital Risk?

Operational resilience extends beyond cybersecurity, it reflects an organization's ability to design a technological architecture that is resilient, controllable, and verifiable. In this context, technology infrastructure choices become strategic decisions. They are not only about performance or scalability but also about the degree of control, auditability, and sustained operational resilience that an organization can ensure over time.

From regulatory framework to operational architecture

Implementing DORA goes beyond internal policies and controls. It requires architectural decisions aligned with operational resilience principles, including controllability of infrastructure and management of third-party risks.

Selecting ICT providers is therefore a strategic choice. Organizations must evaluate not only technological performance but also the provider's ability to support auditability, governance, and resilience requirements defined by the European regulatory framework.

CHAPTER 09

Aruba and operational resilience in the context of DORA

When selecting ICT partners, organizations must complement traditional technology assessments with risk governance considerations. Financial institutions are expected to demonstrate not only system security but also the transparency, auditability, and resilience of the entire digital supply chain.

In this landscape, **Aruba positions itself as a European technology partner capable of supporting organizations operating in regulated environments.** By offering infrastructure solutions designed for compliance, continuity, and transparency, Aruba helps reduce operational complexity and strengthen the controllability of ICT systems, enabling financial institutions to meet DORA's operational resilience objectives.

1. Integrated Digital Infrastructure

Aruba is one of Europe's leading operators capable of delivering a fully integrated digital services ecosystem, which includes:

- **proprietary data centers** certified in compliance with ANSI/TIA Rating 4 standards;
- **cloud services and distributed infrastructure** across European regions;
- **cybersecurity services**;
- **qualified trust services** under the eIDAS Regulation;
- **encryption solutions** compliant with PSD2 requirements;
- **connectivity and interconnection services**.

Within the group, **Certification Authorities Actalis** and **Aruba PEC** provide the certified foundations supporting trust services, including large-scale deployment of certified email (PEC), digital certificates, and digital signatures.

This vertical integration simplifies ICT supply chain management and enables organizations to more effectively address Third-Party Risk Management (TPRM) obligations as required by DORA.

2. Auditability & Operational Collaboration

DORA requires financial institutions to demonstrate the controllability of ICT providers and the ability to conduct technical and organizational verifications. **Aruba undergoes continuous internal audits as well as independent third-party assessments performed by accredited auditors and certification bodies.**

Additionally, Aruba actively supports client-led assessments, audits, and supervisory inspections, ensuring a high level of operational transparency. This approach enables organizations to meet regulatory control requirements more effectively, providing evidence of compliance and reinforcing trust in critical ICT operations.

3. Contractual Flexibility for Enterprise Clients

Unlike the highly standardized contract models of some global providers, **Aruba offers customizable contractual solutions for enterprise clients.** Organizations can request specific clauses tailored to their operational, compliance, or ICT risk governance needs. This flexibility facilitates the development of agreements that are fully aligned with regulatory requirements and the organization's operational resilience objectives.

4. A Single Point of Contact for Infrastructure and Operations

In addition to infrastructure, trust, and cloud services, **Aruba provides managed services for operational oversight.** This model allows organizations to reduce fragmentation across multiple technology vendors, maintaining a single point of contact for infrastructure, platforms, and operational management. Simplifying the ICT supply chain in this way is a key enabler for effective third-party risk management.

5. Governance and European-Based Infrastructure

Aruba's corporate structure and legal status, fully governed under European Union law, ensure that strategic and operational control over services remains exclusively within the European jurisdiction. This framework enables Aruba to guarantee geographic and legal data localization, exclusive control over data processing and storage operations.

- compliance with European Regulatory Frameworks – Aruba ensures adherence to key EU regulations, including GDPR, NIS2, DORA, and others;
- independence from Extraterritorial Legal Conflicts to non-EU laws with territorial effects, such as the US CLOUD Act, Patriot Act, or Chinese Cybersecurity Law;
- protection of European Users' Rights – EU authorities enforce accountability and oversight.

Aruba's corporate structure and legal status, entirely under European Union law, guarantee that strategic and operational control of services remains exclusively within EU jurisdiction.

In a context where digital sovereignty is becoming increasingly central to technology strategy, **European governance of ICT infrastructure represents a distinct advantage for regulated organizations.** A provider truly oriented toward digital sovereignty can support organizations not only in regulatory compliance, but also in developing a more autonomous and resilient IT governance model.

6. Industrial Strength

Aruba is today one of Europe's leading private digital infrastructure providers, with recognized expertise in mission-critical and regulated cloud services. The group's financial solidity and sustained organizational growth provide a reliable foundation for institutions that must guarantee long-term operational continuity.



CHAPTER 10

The new currency of financial trust

In today's digital financial markets, trust is no longer measured solely by balance sheets or capital strength. Increasingly, it depends on an organization's ability to ensure operational continuity, maintain control over technology infrastructure, and manage digital risk transparently.

Key factors, such as demonstrable continuity, data governance, mitigation of concentration risk, and infrastructure auditability, have become essential components of trust in the financial system. Institutions that approach DORA not just as a regulatory obligation but as an opportunity to strengthen operational resilience can enhance their credibility with clients, investors, supervisory authorities, and international partners.

Operational resilience is therefore emerging as a critical competitive differentiator in the digital financial market. It is a governance tool that reinforces stability, reliability, and confidence in increasingly complex technological environments.

This is precisely where **experienced, methodical, and visionary technology partners add value**, helping organizations transform regulatory compliance into a strategic advantage.

CONCLUSIONS

Priority actions

The entry into force of DORA marks a shift from a formal compliance approach to a model of demonstrable operational resilience.

Underestimating the role of the management body or overlooking the complexity of the ICT supply chain exposes organizations not only to regulatory sanctions but, far more critically, to operational and reputational risks.

Financial institutions that can demonstrate full control over their infrastructure while achieving regulatory compliance will also strengthen their competitive positioning. Organizations that select partners capable of integrating security, risk management, operational support, and digital sovereignty principles will be best prepared to navigate the evolving landscape.

In the new normal of cybersecurity, it is no longer sufficient to own the right tools; organizations must use them effectively, responsibly, and aligned with business objectives.

Strategic Gap Analysis

Validate the alignment of existing ICT frameworks with the new Regulatory Technical Standards (RTS).

Contractual Hardening

Update ICT vendor agreements to include clauses ensuring transparency, auditability, and enforceable exit strategies.

Managing Risk in the ICT Supply Chain

Reducing concentration risk requires a structured approach to ICT supply chain management and a thorough evaluation of technology providers. Regulatory compliance is rapidly evolving from a mere legal obligation into a structural driver of competitiveness. When trust is embedded in the technological architecture,

organizations can innovate faster, enter new markets with confidence, and provide supervisory authorities with clear evidence of the robustness of their operational models.

DORA represents a pivotal milestone: operational resilience moves beyond a simple compliance requirement to become a core capability enabling financial institutions to operate securely and evolve in the digital market.

Building strategic and collaborative relationships with technology providers is essential. Partners should support organizations not only on a technical level but also in consulting, operational management, and governance.

The architectural decisions organizations make today, regarding infrastructure, data management, and technology vendors, will determine their freedom of action and flexibility in the future.

Operational resilience and concentration risk management are therefore part of a broader strategic imperative: preserving long-term technological governance, a central element of the concept of strategic control.

About Aruba

Aruba, founded in 1994, is Italy's Cloud Champion and one of Europe's leading providers of digital infrastructures and platforms based on proprietary assets. The company designs and manages the entire technology stack: from the design and construction of data centers to cloud platforms, from trust and cybersecurity services to connectivity and software solutions that support digital strategies and AI-based applications.

With entirely Italian capital, Aruba serves 16 million users from over 100 countries and operates an infrastructure distributed across 8 data centers, hosting thousands of customers' IT infrastructures.



Copyright © Aruba. All rights reserved.

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it