



DORA: Impact on Swiss companies

Executive Summary

DORA (Digital Operational Resilience Act) is an **EU regulation** on operational resilience in the **financial sector**. It defines what financial institutions must have in place organisationally and technically so that cyber attacks, system outages and issues at their IT service providers do not disrupt operations. It requires verifiable evidence rather than statements of intent.

DORA often applies to companies in Switzerland, even if they are not directly regulated in the EU. Typically affected are:

- Swiss entities that are part of EU groups (including group or internal IT/shared services)
- Swiss service providers delivering ICT services to EU financial institutions
- Swiss providers in supply chains where EU customers pass down DORA requirements contractually

DORA has been in effect since 17 January 2025, shifting the focus from “We are in principle resilient” to “We can **prove resilience**.” This requires clear responsibilities, robust incident management with reporting capabilities, a structured testing program, and consistent governance of third parties, including exit and concentration risks.

A practical starting point is an implementation program aligned to the **DORA’s five pillars**, complemented by **continuous vulnerability management and realistic testing**. Crowd-based security (for example, VDP/bug bounty programs) strengthens this approach in a targeted way: with a clearly defined test scope, structured assessment and prioritised remediation, including verification of fixes.

What is DORA?

DORA (Digital Operational Resilience Act) is an **EU regulation** (Regulation (EU) 2022/2554) on digital **operational resilience in the financial sector**. It defines a harmonised framework for ICT risk management and digital resilience and sets requirements for managing ICT third parties (especially cloud providers).

DORA’s five pillars are:

- ICT risk management
- Incident management & reporting
- Resilience testing, incl. Threat-led Penetration Testing (TLPT)
- Third-party risk management
- Information sharing (optional)

DORA is about **operational discipline and demonstrable evidence**: clear processes, defined responsibilities, and a recurring cycle of testing, remediation, and verification. This requires strong governance and accountability at Board and Executive Management levels.

Am I affected?

- EU link:** Part of an EU group / EU subsidiary / EU-regulated environment
- EU customers:** providing ICT services to EU financial institutions
- Supply chain:** DORA clauses in contracts, audits, exit requirements

What does DORA mean for companies in Switzerland?

DORA is EU law, but in practice its requirements often extend into Switzerland. The key question is whether a company supports EU-regulated financial entities or is part of a relevant supply chain or group structure. In many cases, DORA becomes relevant through contractual obligations, audit requirements, and operational evidence expectations.

Three typical scenarios

1) EU group / EU subsidiary / EU-regulated environment

Swiss entities that are part of an EU-regulated group are often included in DORA programs, especially when central IT or shared services are delivered from Switzerland. What is typically expected are consistent standards, clear responsibilities, documented processes, and robust evidence (for example testing reports, incident records, remediation documentation).

2) Swiss ICT service providers for EU financial institutions

If Swiss providers deliver ICT services to EU financial entities (for example SaaS, managed services, cloud services, development and operations), DORA requirements are often reflected in contracts. Typical expectations include audit rights, specific security and reporting obligations, requirements for vulnerability management and business continuity and recoverability capabilities.

3) Supply chain / subcontractors

DORA can also be relevant for subcontractors in a supply chain. EU financial entities must actively manage dependencies and third-party risks. As a result, requirements are often passed on through multiple tiers, including transparency on subcontractors, incident obligations, minimum controls and exit provisions.

What is new?

- **Evidence instead of intent:** processes, controls, and responsibilities must be documented in a traceable way and demonstrable in day-to-day operations.
- **Programs instead of one-off measures:** testing, vulnerability management and remediation are expected as recurring cycles.
- **Third parties as a resilience topic:** contracts, audit rights, exit capability and concentration risk are increasingly scrutinized.
- **Resilience, not only security:** stable operations, recovery and crisis readiness are explicitly included.

DORA in practice: what companies need to demonstrate

DORA's impact in Switzerland is felt most directly when EU customers request proof of compliance. Not as theory, but as a practical checklist: which services are critical, how do we test, how do we remediate vulnerabilities, how do we manage third parties. The artefacts below are common denominators across many DORA requirements in practice.

1) Service and dependency inventory (critical services)

Documentation of which services are "critical," what they depend on (systems, data, interfaces, providers), and which recovery objectives apply (for example RTO and RPO).

2) Governance and responsibilities

Clear roles, escalation paths, and regular reporting to the Board and Executive Management, including accountability for risk acceptance and prioritisation of measures.

3) Incident Management including reporting capability

Runbooks, classification, communication paths, and the ability to provide relevant incident information in a timely and structured way (internally and externally).

4) Risk-based testing program including vulnerability and retest evidence

A recurring test plan for critical services linked to vulnerability management: prioritisation, remediation, retesting, and evidence. Depending on applicability, this can also include Threat-led Penetration Testing (TLPT).

5) Third-party register plus contractual and exit components

An overview of relevant providers (including subcontractors and criticality), plus minimum contractual elements: audit rights, incident obligations, SLAs, exit and portability.

6) Evidence pack (audit ready)

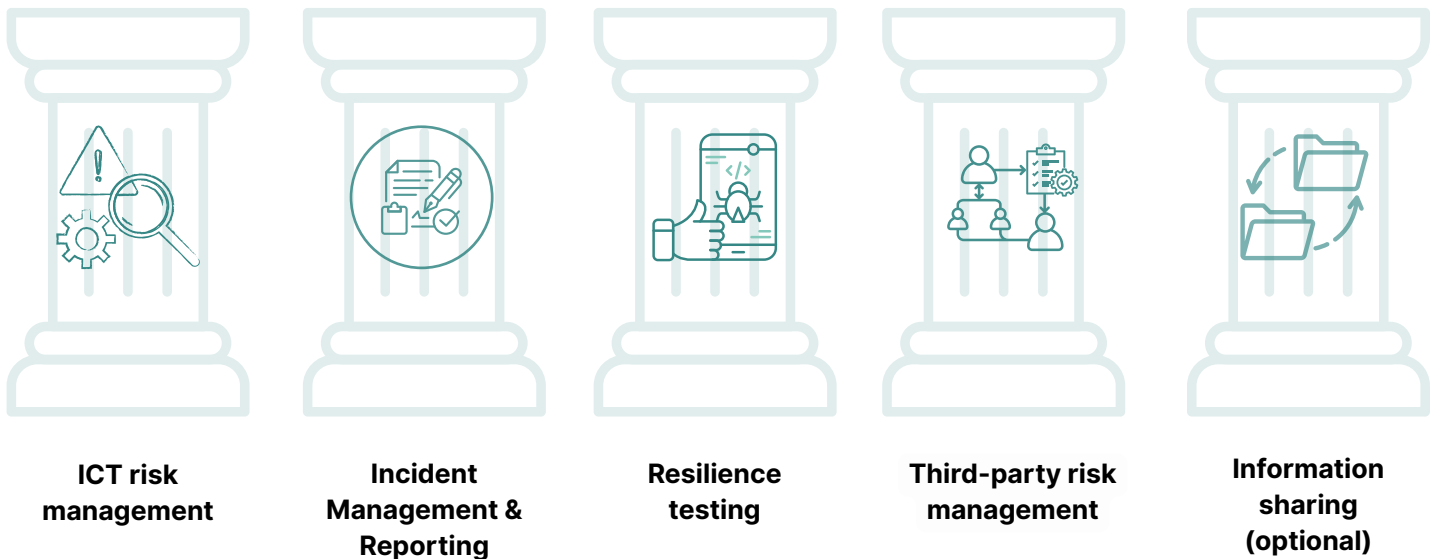
A structured evidence repository that makes decisions, tests, results, and improvements traceable (not only policies, but also how they are implemented and operated).

Typical documents and outputs used as evidence

- **Critical services:** service inventory, dependencies, RTO and RPO, recovery tests (evidence)
- **Third parties and contracts:** security annex, audit rights, incident obligations, subcontractor rules, exit and portability
- **Incident management capability:** runbooks, escalation matrix, exercise records (tabletop), lessons learned
- **Test reports and retests:** current report (pentest, red team, vulnerability assessment, vulnerability scanning), vulnerability status, retest records
- **Vulnerability management:** prioritisation, remediation cycle, analysis of vulnerability exposure time (aging)
- **Continuous testing as a complement:** VDP or bug bounty program scope, rules, triage process, example report

The five pillars of DORA

DORA structures digital operational resilience into five pillars. Each pillar requires not only rules, but evidence that processes work, are tested, and are continuously improved.



Why these five pillars?

ICT risk management

To make risks along critical services visible early, support sound decisions, and keep operations manageable even during disruptions.

Incident Management & Reporting

So incidents can be quickly assessed, handled in a controlled way, and documented in a way that makes impacts, actions taken, and lessons learned traceable.

Resilience testing (including Threat Led Penetration Testing, TLPT)

To validate protective measures against realistic attack and outage scenarios, and to ensure vulnerabilities are not only found but also remediated and verified. TLPT is particularly relevant for certain financial entities or risk based situations.

Third-party risk management

To prevent dependencies on service providers from becoming a single point of failure by ensuring resilience across the supply chain through contracts, audit rights, and exit capability.

Information sharing (optional)

To translate threat intelligence faster into concrete protection and response measures, and to avoid each organisation reacting in isolation.

How crowd-based security supports DORA in practice

DORA shifts the focus from one-off tests to a recurring, demonstrable improvement cycle along critical services: test, prioritise, remediate, verify. In crowd-based security approaches such as bug bounty or vulnerability disclosure, external security researchers report vulnerabilities within clear rules and a tightly defined test scope. The diversity of perspectives and specialisations often helps surface gaps earlier, while triage and verification ensure consistent, traceable outcomes.

Why this approach is particularly effective under DORA



Continuity instead of a snapshot

Periodic tests naturally provide a point-in-time view. Crowd-based security approaches, such as bug bounty programs, can bridge the time between test cycles and make changes in cloud environments, releases, and configurations visible earlier.



Demonstrable proof through standardised processes

DORA expects operational discipline rather than one-off actions. A structured setup produces recurring artefacts: validated vulnerabilities, documented fixes, and verified retests. This makes resilience demonstrable in day-to-day operations.



Focus on critical services

The value is not created by “more testing,” but by targeted testing where outages cause the most harm. Crowd-based security can be scoped to clearly defined critical services and therefore supports the DORA logic.



Quality and efficiency in vulnerability management

In practice, resilience often fails because remediation is not driven through consistently. Triage and quality control filter duplicates and false positives, prioritise relevant vulnerabilities, and enable a clear recurring process including retest evidence.



A stronger basis for audits and customer requirements

In Switzerland, DORA often take practical effect through EU customers. A controlled setup makes it easier to demonstrate that testing and remediation work through consolidated reporting, metrics, and retest evidence.

DORA requires a robust resilience testing program, including procedures for prioritising, remediating, and validating vulnerabilities. This includes coherent vulnerability and patch management, as well as clear processes for **responsible vulnerability communication**.

DORA Quick Check

Question	Yes	Partly	No
Critical services: Have you clearly defined critical services including dependencies (systems, data, providers)?			
RTO/RPO & Recovery: Are recovery objectives documented and tested regularly?			
Governance: Are responsibilities (Board, Executive Management, CISO or IT, procurement) and escalation paths clear?			
Incident Readiness: Do you have runbooks, a communication plan, and exercises (tabletop) including lessons learned?			
Test program: Is there a risk-based, recurring test plan for critical services?			
Vulnerability process: Are prioritisation, remediation, retesting, and evidence standardised (including exposure time)?			
Third-party register: Do you maintain a provider register including criticality, subcontractors, and concentration risks?			
Contractual and exit components: Are audit rights, incident obligations, SLAs, and exit or portability contractually defined?			

Interpretation (rule of thumb):

0–2x “No”: **Good basis.** Keep evidence and cycles clean and consistent.

3–5x “No”: **Action needed.** Prioritise critical services, incident readiness, fix and retest.

6+ x “No”: Significant gap. Define scope, governance, and set up a structured program.


Note: “Partly” counts as “No”, unless it is demonstrated as recurring and evidence-based.


With GObugfree, you establish a recurring testing and remediation cycle with triage, reporting, and retest evidence, focused on critical services.

Start DORA implementation pragmatically

- Continuous testing
- Triage and quality
- Evidence and retesting

Badenerstrasse 281, 8003 Zürich | +41 58 255 04 30 | hello@gobugfree.com

 @GObugfree AG

 #gobugfree

