DECISIONFOCUS

SOLUTION BRIEF

DORA

Digital Operational Resilience Act compliance, evidenced end to end



DECISIONFOCUS

Compliance you can evidence. Resilience you can govern.

DORA is prescriptive. The register of information, supply chain and subcontractor detail, incident classification and reporting deadlines must all be demonstrated in the regulator's format and timescale, with an ICT risk management framework the management body is accountable for behind them. Decision Focus turns those obligations into a live, maintained record rather than an annual spreadsheet exercise.



THE SCALE OF THE TASK

Do not underestimate DORA

Financial institutions have had to demonstrate compliance with DORA since 17 January 2025. Its requirements largely align with existing regulation and good practice, but even operationally resilient and ISO 27001 compliant entities are surprised by the depth of its prescriptive detail.

The layers of technical detail within the Regulatory Technical Standards should not be underestimated. 2 requirements in particular oblige most organisations to establish new processes, and to maintain them continuously.

SIGNIFICANT OBLIGATION 1

Incident impact assessment and reporting

DORA sets a specific method for assessing incident impact, classifying it against materiality thresholds and reporting to the competent authority within fixed windows. Detection, analysis and the initial, intermediate and final reports must all be evidenced.

SIGNIFICANT OBLIGATION 2

The register of information

DORA defines in detail the information you must hold on ICT third party suppliers. You have to show the correct information is held, that it is current, and how it affects the risk ranking of each arrangement, in a prescribed submission format.



THE DORA FRAMEWORK

Five pillars, one platform

DORA - Regulation (EU) 2022/2554 - is directly applicable law across the EU, underpinned by technical standards that set out the criteria, templates and instructions financial entities must follow. It applies to more than 20 categories of financial entities, from banks and insurers to payment institutions and crypto-asset service providers, and reaches EU branches of third-country firms as well as the critical ICT providers that serve them.

01

ICT risk management framework

ERM

Govern ICT risk with management body accountability, identify assets and dependencies, protect, detect, respond and recover, and review the framework itself - with evidence at every step.

02

ICT incident management

ERM, OP RES

Establish detection and logging, undertake cause and impact analysis, apply RTS compliant materiality assessment and reporting, and manage the lifecycle from detection through remediation to closure

03

Digital operational resilience testing

OP RES

Run the full testing programme - vulnerability assessments, scenario tests, penetration testing and TLPT where designated - annually against critical systems, remediate findings and evidence the cycle.

04

ICT third-party risk management

TPRM

Maintain the ICT third-party register, apply DORA criteria in selection, onboarding and monitoring, enforce contractual security clauses, assess concentration risk, map subcontracting chains and maintain tested exit strategies.

05

Information and intelligence sharing

ISMS

Collect and share cyber threat intelligence, collaborate with industry peers to strengthen resilience, and report on participation

Delivering business benefits

DORA

Retire the Excel register

Replace spreadsheet-based DORA registers with a live, interactive register that populates itself from data already held in the platform.

Regulator-ready export

One button produces the ZIP package with every CSV sheet, encoding and validation rule in the format competent authorities expect.

Enter data once

Suppliers, contracts, services and risks held in TPRM, Operational Resilience and ERM flow straight into the DORA register.

Faster major incident triage

Configurable tolerance rules calculate whether an incident meets DORA major incident thresholds, protecting the 4 hour reporting window.

Unlimited users

Organisation-level licensing means anyone can report an incident, attest to a policy or open a dashboard, with no seat counting to discourage reporting.

Configured around your processes

No-code configuration mirrors the way your teams already work, so adoption is quicker and change management is lighter.

Pre-built DORA content

4 policies, 25 procedures, 2,500+ mapped controls and a full mapping of the regulation and its RTS, so you start from templates rather than a blank page.

Regulatory maintenance included

When authorities revise requirements or add fields, we update the platform so your export continues to meet the validation rules.

Lower consultancy spend

Maintain the register and manage submissions in-house, instead of paying recurring fees to an external partner for every update.

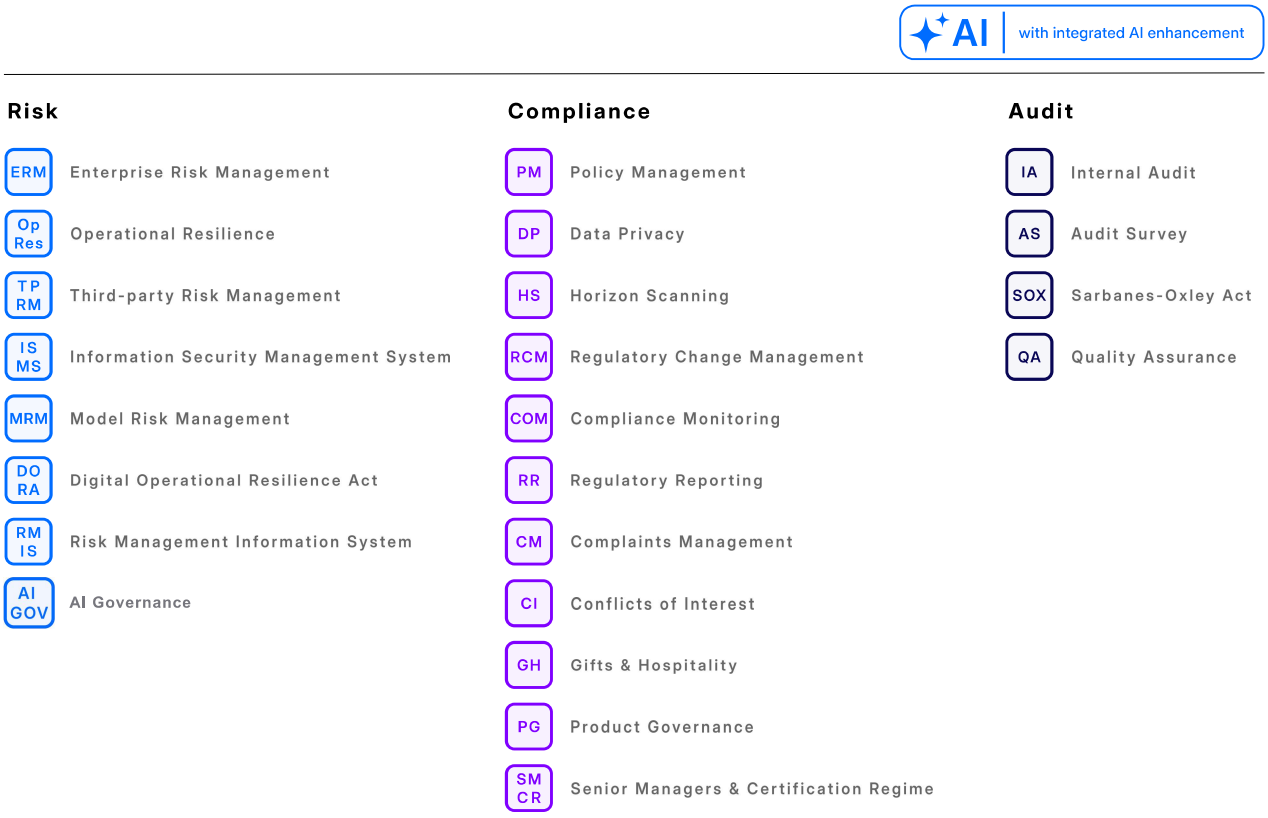
ONE UNIFIED PLATFORM

One cohesive compliance platform
Covering every DORA demand

5 modules collectively cover your DORA obligations: Enterprise Risk Management, Operational Resilience, Third Party Risk Management, Information Security Management and Policy Management. All of them run on the same integrated assurance platform and share a single repository, so the solution serves every stakeholder at once.

Add the rest of your governance, risk and compliance requirements as they arise. Our agile no-code platform adapts to your frameworks and processes, with no burden on your IT resources, so implementation is measured in weeks rather than months.

One unified platform





Enterprise Risk Management

Enterprise Risk Management gives you the oversight needed for effective ICT risk taking and mitigation, working from a single source of truth with dashboards, structured reporting and real-time metrics.

ADDRESSES PILLARS 1 AND 2

Centralised incident logging, analysis and reporting, following the specific method DORA sets out for analysing the impact of an incident.



Operational Resilience

Establish and continually validate your ability to operate through disruption: rank products and services, determine important business services, then map dependencies, tolerances, recovery strategies and testing.

ADDRESSES PILLARS 2 AND 3

Scenario testing against severe but plausible disruption, with the incident management needed to respond when a critical situation materialises.



Third Party Risk Management

A central repository of third parties and their risk, covering the whole lifecycle from due diligence to contract management and SLA oversight, with supplier data gathered through a secure portal.

ADDRESSES PILLAR 4, AND THE REGISTER OF INFORMATION

Holds the supplier information DORA requires, evidences that it is current, and shows how it affects the risk ranking of each arrangement.



Information Security Management

Define and manage the controls that protect the availability, authenticity, integrity and confidentiality of your ICT assets - the four security objectives DORA sets - supporting ISO 27001 and mapping each control to the protection and prevention measures of Article 9 and its RTS, so one control set evidences both the certificate and the regulation.

ADDRESSES PILLARS 1, 4 AND 5

Used with Third Party Risk Management, it covers both third party and wider ICT risk, including the sharing of cyber threat intelligence.



Policy Management

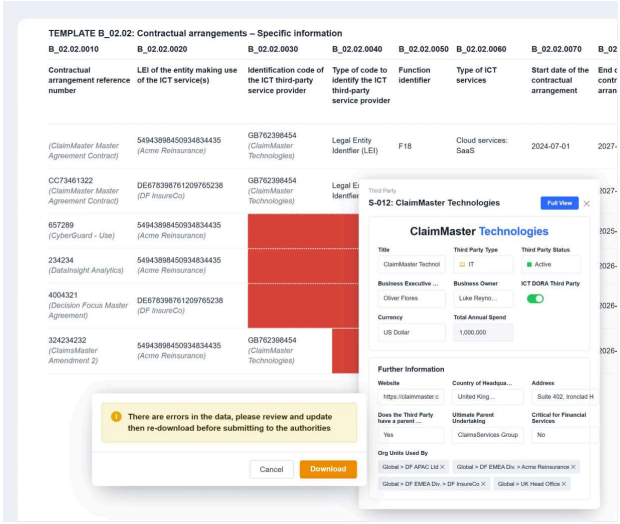
Govern board policies and employee attestations, with readership groups, dashboards for attestation oversight, policies connected to controls, and managed approvals, versions and change history.

ADDRESSES ALL PILLARS

Documenting policies, showing adherence to them and managing policy change is required across DORA, much of it without a specific reporting format.

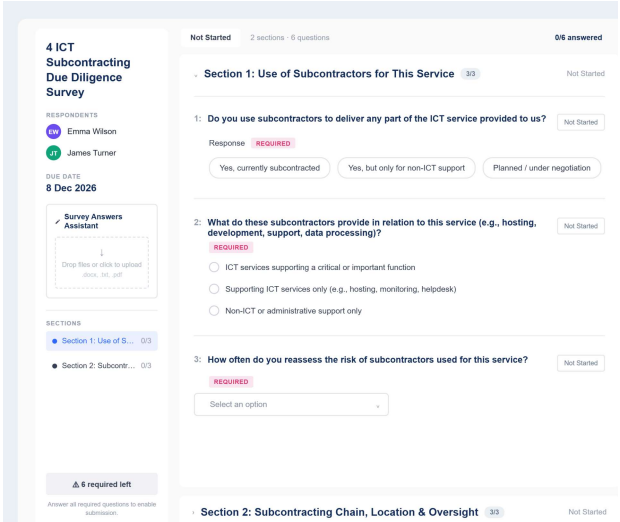
DORA FEATURES

Built for the register. Built for the whole regulation.



Register of information

An interactive, spreadsheet-like view populates every required tab, covering entities, contracts, functions and assessments, from live platform data, and highlights the fields still missing. One click exports the complete register in the exact ZIP format competent authorities require, with all CSV sheets, encoding, code translations and validation rules applied.

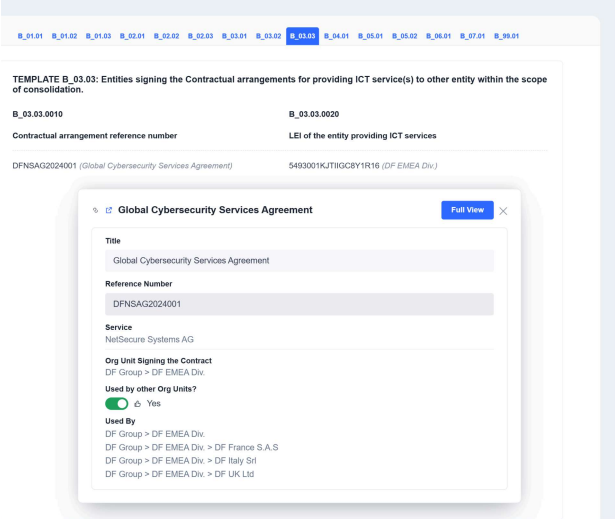


Third party oversight

Third parties complete questionnaires, upload declarations and hold threaded discussions in a secure portal, with automated notifications throughout due diligence - so ongoing oversight of every ICT arrangement runs on current data supplied by the provider, not last year’s spreadsheet.

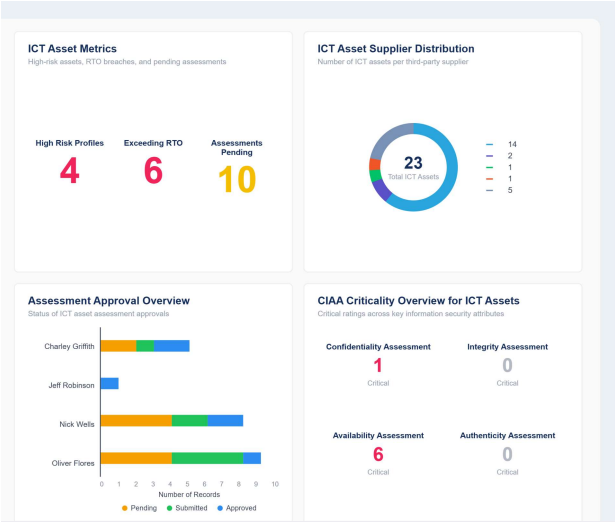
Contract management

DORA and its RTS set out what every ICT contract must contain and how it must be recorded. Intercompany SLAs and intragroup contracts are supported within the register and flagged separately from third party contracts.



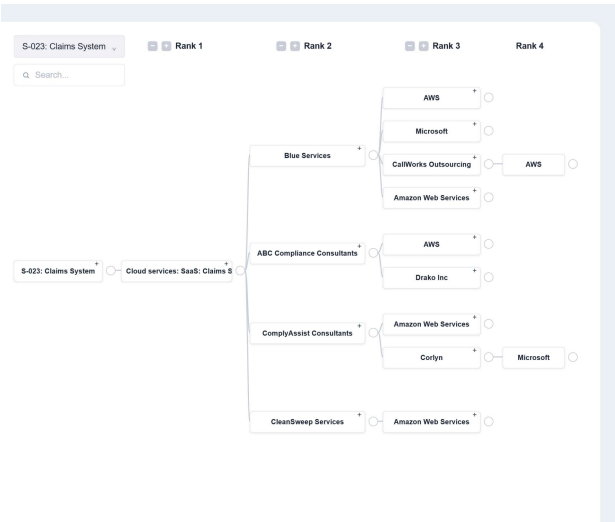
ICT asset inventory

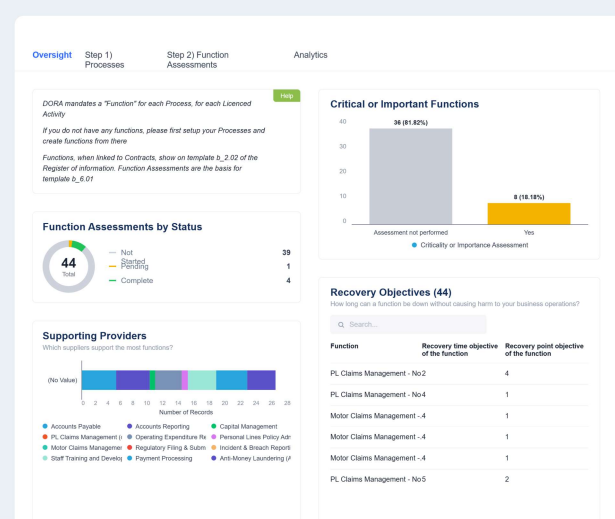
Maintain the inventory of ICT assets and dependencies that Article 8 identification rests on, classified by criticality and linked to functions, suppliers and risks. When an asset changes, everything downstream - risk assessments, testing scope, the register - sees it.



Fourth party management

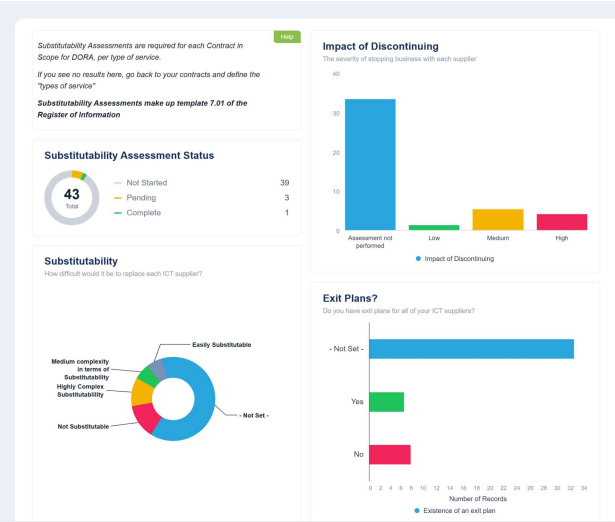
Map the supply chain behind each ICT service, showing which sub-contractors sit behind every service component. Ranked chains align directly to the Register of Information (DORA Article 28(3), template B_05.02), where rank 1 is your direct provider and every rank above is a sub-contractor.





Critical and important functions

Capture and classify critical and important functions in line with DORA, linked to licensed activities, entities, suppliers and function assessments.



Substitutability assessments

A built-in workflow covers substitutability scoring, the impact of discontinuing a service and exit planning for every arrangement in scope - populating register template B_07.01 while holding the documented, tested exit strategy Article 28(8) requires behind each yes.



Resilience testing programme

Plan and evidence the full Article 25 testing programme: vulnerability assessments, scenario-based tests, network security reviews and source code assessments, each scheduled against critical functions. Findings flow into remediation actions with owners and deadlines, so the annual testing obligation is a managed cycle rather than a scramble before the audit.

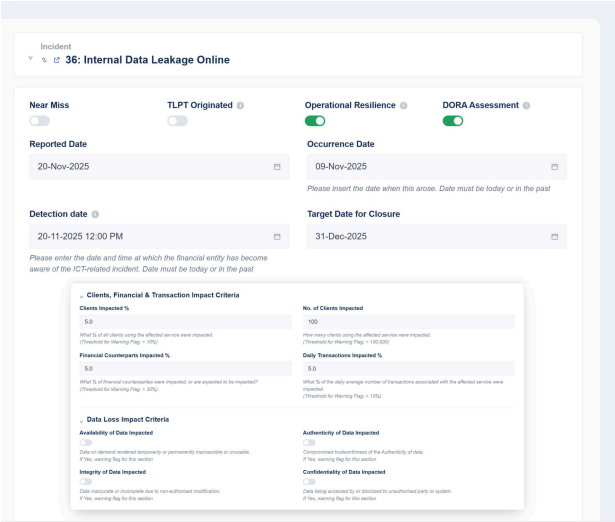
Threat intelligence participation

Register your information-sharing arrangements, log intelligence received and actioned, and evidence participation in sharing communities. Article 45 makes sharing voluntary but expects you to notify the authority when you take part - the platform keeps that record current.



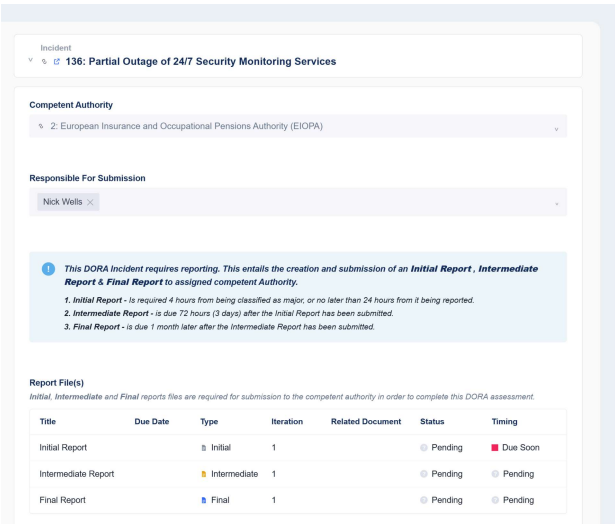
DORA incident

Flagging an incident as a DORA matter opens the additional DORA sections on the same record, with the mandated fields, impact criteria and classification logic applied automatically. Incidents link to risks, controls, third parties and important business services, pulling in maximum tolerable disruption times so major incidents are flagged as the picture develops.



Initial, intermediate and final reports

The 3 mandated report types are generated from the incident record, using configurable templates with approval workflows, assignees and a full audit trail. Once an incident is classified as major, a countdown appears on the record and email and in-app notifications keep the 4 hour initial report deadline in front of the people who own it.



Built by GRC experts, for GRC experts

Decision Focus is built, tested and implemented by GRC experts with decades of experience across industries. We know the challenges you face, the tools you need and how to deliver the results you want.

Decision Focus is an agile, no-code platform that allows organisations to create a tailored GRC solution from more than 20 configurable modules, spanning risk, compliance, audit, governance, regulatory reporting and more.

As a true 'Total GRC' platform, it brings all of your GRC processes into one unified system. At the centre is a focus on lean GRC, to help you eliminate inefficiencies and drive business growth.



Chartis RiskTech100 2025

Chartis RiskTech AI 50 2024

2026 REGTECH 100 www.RegTech100.com

MILESTONE Users Love Us

FALL 2025 High Performer

FALL 2025 EMEA High Performer



DECISIONFOCUS

THE ONLY PLATFORM FOR ALL YOUR GRC

When it comes to GRC, one size does not fit all.

Built to fit your organisation, so you can choose the solutions that matter now and add more later.

See how Decision Focus can support your DORA compliance and ongoing GRC maturity. Get in touch at info@decisionfocus.com to book a demo.