DORA-first

AI-native DORA GRC for IT and compliance teams

GRC = Governance, Risk and Compliance

Turn DORA requirements into executable GRC workflows with AI.

Product: DORA-first

Positioning: AI-native DORA GRC

Core capability: Risk Copilot

What is DORA?

Digital Operational Resilience Act
EU financial-sector resilience regulation

- Financial entities under EU financial supervision must comply
- Mandatory from January 17, 2025
- Covers banks, payment institutions, e-money institutions, investment firms, insurance and reinsurance, trading venues, central securities depositories, fund management, crypto-asset service providers, and other financial entities

Start from the real DORA learning problem of an IT practitioner

I studied DORA carefully, but the real problems started when we tried to operationalize it.

Hard to remember

DORA covers ICT risk, third parties, incidents, BCP/DR, recovery targets, and many other obligations. Memory is not reliable.

Manual review is slow

Architecture, cloud assets, vendors, policies, and evidence are scattered. Manual judgment is slow.

High learning cost

Not every IT teammate will study regulation deeply. They need learning and execution that fit technical scenarios.

Lessons learned: the hard parts are sources, mapping, and data quality

Limits of existing tools

Field experience shows most existing tools are compliance workflow platforms: Vanta handles control status and evidence integrations; SureCloud manages risk, incidents, vendors, and resilience; Formalize structures DORA and generates registers.

Differentiated MVP

Use plug-in APIs to ingest architecture docs, cloud assets, vendor registers, policies, incidents, and BCP materials, then output DORA gaps, evidence sufficiency, issues, and remediation actions.

Dynamic regulatory source base

Start with a structured DORA source base that covers official regulation and supplementary materials. Version updates and source traceability cannot be static.

Obligation tags and controls

Tag obligations at a granular level, define control mechanisms, and connect them to enterprise documents and policies.

Internal data quality

The biggest challenge is not the model itself, but the quality of internal data, documents, assets, and evidence.

Make the risk engine explicit

Do not only show scores and statistics. Explain why it is a risk, what evidence is missing, and which DORA obligation is triggered.

Field experience also shows some companies put 50+ people on ICT risk and gap work. If this can be productized, the scaling value is significant.

The product model abstracted from field experience

> **The product is not a single page. It is a chain: DORA source base → obligation tags → document/evidence graph → AI risk engine → remediation and continuous monitoring.**

1 Level 1: DORA Expert

Retrieve only official sources, answer IT questions, and provide citations, such as ICT third-party subcontracting risk.

2 Level 2: DORA Mapper

Ingest architecture docs, policies, vendor lists, and related materials to produce requirement-to-control mapping.

3 Level 3: Semi-automated Assessor

Consume live or near-live evidence and continuously monitor DORA posture and risk issues.

Formalize: a DORA-focused compliance workspace

Formalize

Turns DORA into structured workflows that are executable, auditable, and submission-ready.

More compliance-team oriented: obligations, tasks, controls, evidence, and registers drive DORA implementation.

Learn the market first, then define differentiation

Core capabilities

Structured DORA obligations
Task and control management
Evidence and policy organization
Register of Information generation
Completeness and consistency checks

Competitor summary

Formalize's strength is not AI or technical architecture analysis. It turns DORA into an executable, submission-ready, auditable compliance workflow.

Weakness / gap

It is more focused on compliance teams and register management. IT teams still need someone to translate architecture, vendors, cloud assets, and evidence into DORA context.

Lesson for us

We cannot build only AI Q&A. We need structured DORA obligations, controls, tasks, and evidence models. Otherwise it looks like a demo, not an operational system.

Our differentiation

Formalize is strong in compliance structure. Our opportunity is Risk Copilot: translating architecture, cloud assets, and vendor evidence into DORA risk, triggered obligations, and remediation.

SureCloud: a signal that DORA becomes GRC

SureCloud

DORA is not a standalone compliance task. It ultimately enters GRC operations.

More enterprise oriented: DORA sits inside risk, incidents, third parties, business continuity, and control monitoring.

Learn the market first, then define differentiation

Core capabilities

Risk management
Third-party risk management
Incident and remediation workflows
Business continuity / operational resilience
Multi-framework compliance and audit trail
AI-assisted GRC workflows

Competitor summary

SureCloud's strength is not a single DORA form. It puts DORA into an enterprise platform for GRC, third-party risk, incident management, and operational resilience.

Weakness / gap

That is not a weakness; it shows DORA's long-term form is GRC. But traditional GRC still requires heavy manual configuration, mapping, evidence judgment, and risk explanation.

Lesson for us

We should become GRC too, but with Risk Copilot. The base model should include frameworks, obligations, controls, evidence, risk, vendors, incidents, and remediation.

Our differentiation

SureCloud validates the platform direction. Our differentiation is serving IT and compliance operations with Risk Copilot that turns technical facts into risk, obligations, evidence gaps, and remediation.

Vanta: automated evidence and continuous compliance

Vanta

Moves compliance from manual evidence collection to integration-driven continuous monitoring.

More automation oriented: connects cloud, code, identity, devices, and vendor systems to continuously check control status.

Learn the market first, then define differentiation

Core capabilities

Pre-mapped controls
Automated evidence collection
Continuous control monitoring
Vendor and risk management
Multi-framework evidence reuse
Policy and report automation

Competitor summary

Its strength is not explaining regulatory detail. It automates evidence collection through integrations, tests, and continuous control monitoring.

Weakness / gap

It focuses more on whether controls pass and evidence exists. DORA-specific risk reason, triggered obligation, and evidence sufficiency may be less explicit.

Lesson for us

We cannot stop at one-off assessment. We need continuous monitoring so evidence, vendors, and asset states keep entering the judgment.

Our differentiation

Vanta is strong in evidence automation. Our opportunity is making Risk Copilot more explicit: why it is a risk, what evidence is missing, and which obligation is triggered.

Product definition: what DORA-first is

> **After pain points, field experience , and competitor analysis, the conclusion is not another chatbot, but a Risk Copilot with DORA GRC platform.**

Product name

DORA-first
The product brand focused on operationalizing DORA.

Positioning

AI-native DORA GRC platform
GRC = Governance, Risk and Compliance.

Core AI capability

Risk Copilot
Aligns regulatory requirements with enterprise data and produces explainable risk judgments.

GRC output

Triggered obligation
Risk reason
Evidence gap
Remediation actions
Audit trail

One sentence: DORA-first uses AI to turn DORA requirements into executable GRC workflows.

The 4 core Risk Copilot capabilities

It is not a chatbot. It is a risk-judgment assistant connecting external regulatory requirements with internal enterprise data.

1. Read requirements

Read external regulatory requirements: DORA, RTS/ITS, regulatory guidance, supplementary materials, and version changes.

2. Understand data

Understand internal data: architecture, cloud assets, vendor evidence, policies, BCP/DR, and incident records.

3. Explain risk

Explain why it is a risk, what evidence is missing, which DORA obligation is triggered, and what remediation comes next.

4. Continuous monitoring

Continuously monitor external regulatory changes and internal data changes, then update risk state, evidence gaps, and remediation actions.

Risk Copilot guardrails

Traceable official sources · Evidence-based judgment · Confidence shown · Human review retained

MVP loop: prove ICT third-party risk first

The first version is not broad. It goes deep on one high-value scenario: ICT third-party risk.

Auto-discover
Identify critical ICT third parties from vendor registers, architecture notes, and cloud assets.

→

Collect evidence
Collect SOC2, ISO, BCP/DR, incident, subcontractor, and related evidence.

→

Copilot judgment
Align requirements and evidence, then judge sufficiency.

→

Risk explanation
Explain why it is a risk, what evidence is missing, and which obligation is triggered.

→

Remediation actions
Generate remediation actions, evidence requests, owners, and follow-up checkpoints.

How the website supports this loop
Risk Copilot demonstrates reading requirements, understanding data, explaining risk, and continuous monitoring; DORA Academy supports team learning and scenario understanding.

Why this can expand into GRC
The same object model can later support incidents, BCP/DR, policies, control testing, audit packs, and multi-framework evidence reuse.

The MVP value is not showing a model. It proves Risk Copilot can enter compliance operations and continuously produce auditable risk judgments and remediation actions.

Milestones: from MVP to multi-framework platform

MVP

Current version

DORA source base
DORA Q&A
Risk Copilot
ICT third-party risk loop
DORA Academy

V0.2

Evidence workflow

Evidence library
Document upload
Task assignment
Audit pack export

V0.3

Continuous monitoring

Cloud connectors
Vendor monitoring
Incident / BCP change monitoring
Compliance status trend

V0.4

Team collaboration

Roles / approvals
Comments
Review history
Dashboard trends

V1.0

Multi-framework GRC

DORA + NIS2
ISO 27001 / SOC2
Common controls
Evidence reuse

Vision: move from one-off compliance checks to continuous regulatory readiness.