USE CASE

DORA evidence that stays current between audits

Aribot builds the ICT risk picture from your architecture and keeps the evidence current as systems change, so the third-party register is never a quarter-end project.

THE PROBLEM

DORA asks a bank or insurer to know its ICT risk and its third parties all year, not once at audit time. The architecture changes every sprint, the register lives in a spreadsheet, and the evidence is assembled by hand when the supervisor asks.

HOW ARIBOT HANDLES IT

1. **Model the systems in scope**
   Upload or draw each system and Aribot generates the threat model, with the controls that close each threat.
2. **Map controls to DORA**
   Each control is mapped once and shows every requirement it satisfies across DORA, ISO 27001 and NIST.
3. **Assess third parties**
   Run vendor assessments in Ayurak Trust and keep the answers beside the controls they support.
4. **Keep it current**
   Connected cloud accounts keep the architecture in step, so a changed system shows up as new risk.

WHAT YOU SEE IN THE DEMO

- Compliance Standards: framework coverage per control
- Threat Modeling: threats per component with the controls that close them
- Ledger Integrity: evidence an auditor can verify

WHO IT IS FOR

Head of ICT Risk

Head of Information Security Architecture

CISO · Chief Risk Officer

WHAT YOU GET

- An ICT risk view built from the real architecture
- Third-party assessments tied to the controls they evidence
- Evidence that builds up as engineers fix things
- One control mapped once, satisfying many frameworks

86%

of finance executives polled weeks after DORA took effect said they were not yet fully compliant

Source: Clear Junction, DORA webinar poll (2025)

DORA · 17 Jan 2025
ICT risk management, resilience testing, a third-party register and incident reporting apply now.

See it: ayurak.com/demos/compliance-standards

€75 per compliance scan · €120 per vendor assessment · €600 per diagram