mondoo

CASE STUDY

CONTINUOUS SECURITY, CONTINUOUS COMPLIANCE

How a long-established European bank made DORA evidence a by-product of the way it runs security, provable on demand.

DORA did not create a compliance problem for Europe's banks. **It created an exposure management challenge.** The institutions that read the regulation as a documentation exercise built frameworks, policies, and registers designed to pass a review.

The ones that read it correctly built something different: a continuous operating model that produces compliance evidence as a by-product of good security. The bank in this case study is in the second group, and Mondoo contributes a foundational capability to that model.

AT A GLANCE

ORGANIZATION: An established European Bank

SECTOR: Regulated universal bank serving private and corporate customers in the EU

SCALE: European bank with a multi-billion-euro balance sheet and an extensive branch network

REGION: European Union

ENVIRONMENT: Roughly 70 to 75 percent on-premises. VMware, Windows, and Linux servers, Windows and Mac endpoints. Core banking is delivered through a shared group IT service provider

SECURITY FUNCTION: Effectively, one head of security, a small team, and external consultants

MONDOO'S ROLE: Central platform for DORA-aligned ICT governance evidence and Continuous Threat Exposure Management (CTEM)

01
THE BANK

A REGULATED BANK THAT RUNS ITS OWN ESTATE

This case study describes an established European bank: a regulated institution with a multi-billion-euro balance sheet and an extensive branch network. It serves private and corporate customers and belongs to a wider banking group whose members share central services and infrastructure.

Unlike many smaller institutes that source most of their IT from the group's shared service provider, this bank runs a large share of its own infrastructure in-house: the full LAN, WAN, and SD-WAN, the complete security stack from end-point to perimeter, data center operations,storage virtualization, and telecommunications. Roughly 70 to 75 percent of that estate is still on-premises, built on VMware with Windows and Linux servers and Windows and Mac endpoints. The security function is lean, with a single head of security supported by a small team and external consultants.

02
THE CHALLENGE

DORA CHANGED THE QUESTION

For the bank's head of security, the dominant threat has not changed: a successful attack, most often ransomware, that stops the business from operating because its systems are no longer available. What changed is the standard he is held to. For banks, DORA takes precedence: it overlaps closely with the broader NIS2 directive in substance, but as the finance-specific rule, it is the one banks follow. Its ICT risk management articles set out in concrete terms what has to be done and to what quality, with an implicit expectation that firms anchor to recognized frameworks such as the ISO 27001 family and NIST, alongside the technical guidance issued by the country's national cybersecurity authority.

The pressure became concrete through the bank's mandatory annual audit. It is carried out not by a Big Four firm but by its external sector auditor, and it includes the

IT audit. The finding ran counter to the transparency and traceability of the ICT risk management process and its handover to operational risk. Too many media breaks between systems, manual, Excel-based workflows where automation should have been in place, and a methodology that a regulator could not trace from one step to the next.

> “You have four spreadsheets, and at some point, something flows into operational risk, and we have no way to follow how you get from A to B. Please explain it.”

THE AUDIT FINDING, AS THE HEAD OF SECURITY DESCRIBES THE REGULATOR’S POSITION

Underneath the finding sat a harder truth about the starting point. The bank had no hardening baselines at all. The metrics in its information security management system were, in the head of security’s words, weak, basic, and few. Key Risk Indicators (KRI) were assembled by hand. None of that would withstand DORA scrutiny, and everyone involved knew it.

03
THE SOLUTION

ONE PLATFORM AS THE HUB

The bank’s head of security describes Mondoo as the central hub, the turntable that everything else feeds off. He frames its value in two halves running off a single source of truth. On the one hand, it provides the ICT governance framework with concrete, up-to-date information from the infrastructure. On the other hand, it gives the operational team a risk-weighted way to prioritize patch and vulnerability management, with a Jira integration carrying remediation into the existing workflow. Crucially, the frameworks and their controls are built into the platform as traceable code, so there are no mapping tables to build and no derivations to write up by hand.

HARDENING, INVERTED

The clearest illustration is hardening. With no baselines to start from, the team inverted the usual order: take what the platform checks, declare that the requirement, then validate each check against the real environment. Where a control genuinely cannot be met because a group provider has hard-configured a setting the bank does not control, for example, a minimum password length fixed at 10 against the CIS Level 2 benchmark of 13, the check is removed with a documented justification. That keeps the bank regulatorily compliant, and the posture picture honest at the same time. From the gap, the team can risk-weight its standing, derive remediation actions, and report on it regularly and in a traceable manner.

METRICS AS A BY-PRODUCT

The same discipline runs through the metrics. KRIs and KPIs now flow automatically from Mondoo into the ICT risk management process and the ICT risk register. Each metric has a defined profile: how it is composed, what the target value is, and how it is collected, in the same automated, standardized, traceable way every time. The work that used to be manual is now a by-product of the platform doing its job.

Agentic automation is what lets this run at the scope and pace DORA assumes, but he is candid that judgment cannot be automated away. Deciding which checks apply to a specific environment, validating results, and reasoning about exceptions is work that no tool and no AI can remove. That is not a weakness of the model. It is the control. The platform produces evidence at scale, and a human remains accountable for what it means and for operational change decisions, which is exactly the traceability supervisors require.

04
ONBOARDING & LESSONS

START WITH ONE ASSET TYPE

Getting systems and infrastructure into the platform was, in his words, a piece of cake. The real effort, as with any serious tool in the cyber and compliance space, lies in tuning: deciding which benchmarks apply to which systems, validating individual checks, and scoping the results to the environment. His advice to new customers is to resist the urge to onboard everything at once. Start with one asset type; Windows endpoints are a sensible first target. Understand what the platform is telling you, then expand. Trying to do it all at the start is how you end up overwhelmed.

The campaign is honest, not safe, so the friction belongs here too. Because the agents pull updates from the internet, the group endpoint protection objects, so the bank cannot use near-real-time auto-update and instead pushes updates through standard software deployment on a slower cadence. It works, but it is not automatic. There was also a one-off reporting issue in which reports were not generated or handled as part of the normal support process. And Mondoo is not a full end-to-end GRC platform, nor does it try to be. What stood out on the positive side were the pace of development, new integrations, and consistently short response times. Regarding the customer-vendor relationship, the head of security is unequivocal: super satisfied.

05
RESULTS

FROM FINDING ISSUES TO FIXING THEM

The measurable outcome is a strong downward trend in identified vulnerabilities, noted in a prior review, driven by the team acting on what the platform surfaces. That is the part of exposure management that matters most: the move from finding issues to fixing them, closing the gap between discovery and remediation rather than just reporting on it.

> IN MY VIEW, EVERY BANK SHOULD BE RUNNING IT.
>
> - HEAD OF SECURITY

The structural outcome matters as much: a single methodology and a single platform replacing splintered, media-broken workflows, with one complete view across the whole landscape and traceable evidence on demand. The consolidation is already underway, with the classic vulnerability scanner lined up for retirement, tool sprawl reduced, dedicated asset management handled alongside, and compliance and exposure evidence centered on Mondoo.

1+	**70–75%**	**1** platform
Security headcount — one head of security, plus consultants — running the model	On-premises estate brought under continuous assessment	One methodology replacing four spreadsheets and media-broken workflows

> When the auditor comes, I press the button and say: here, this is how it looks, this is how it looked last week, this is how it looked four weeks ago, this is the trend, this is what we do and how we do it."
>
> - HEAD OF SECURITY

06

DORA MAPPING

HOW MONDOO CONTRIBUTES TO MAINTAINING DORA COMPLIANCE

No single platform evidences every requirement of DORA. At this bank, Mondoo is the platform for the continuous evidence and exposure-management requirements at the heart of the regulation, and it contributes evidence to the requirements adjacent to them.

PRIMARY	
ART. 9	Protection and prevention
ART. 10	Detection of exposures, misconfigurations, posture drift
ART. 24	General testing requirements
ART. 25	Testing of ICT tools and systems

SUPPORTING	
ART. 5-6	Operational metrics and KRIs feeding the ICT risk-management framework
ART. 13	The data layer behind lessons learned
ART. 28	Third-party posture, where surfaceable

ABOUT MONDOO

Leading industry analysts now describe exposure management as moving from visibility to action: closing the gap between discovering an exposure and actually neutralizing it, rather than stopping at a prioritized report. They frame this shift as preemptive exposure management, the action-oriented evolution of CTEM. This bank is what that model looks like within a regulated, heavily on-premises EU bank: continuous assessment, business-context prioritization, and remediation, all tracked and documented on a single platform.

DORA CANNOT BE PASSED. IT HAS TO BE PROVEN.

Documenting compliance is the floor; the ability to robustly fix and mitigate risks, continuously and at scale, is what builds operational resilience. This bank is proof that the exposure-management operating model is achievable in a real, regulated environment, with a security headcount of effectively 1 plus consultants. Mondoo closes the half of the gap that documentation cannot, and turns evidence into resilience. In that order.