NEXERIS

CASE STUDY

Compliance & Audit Readiness

DropStream: ISO 27001 End-to-End Certification

This case study demonstrates how Nexeris helps fast-growing SaaS companies translate complex, daunting security frameworks into clear, practical roadmaps. It highlights how we establish a robust, audit-ready security posture that accelerates sales cycles and reinforces trust with enterprise buyers.

CLIENT

DropStream (SaaS e-commerce integration platform)

INDUSTRY

E-commerce, Supply Chain Logistics, Software as a Service (SaaS)

ENGAGEMENT TYPE

End-to-End ISMS Development, Risk Assessment, Mandatory Internal Audit, and Audit Representation (Stage 1 & Stage 2)

© 2026 Nexeris. All Rights Reserved.

OVERVIEW & THE CHALLENGE

End-to-end ISO 27001:2022 certification delivered for a lean, engineering-first SaaS team.

CLIENT PROFILE

CLIENT
DropStream

INDUSTRY
E-commerce, Supply Chain Logistics, Software as a Service (SaaS)

COMPLIANCE LEVEL
ISO/IEC 27001:2022 Certification

KEY ACHIEVEMENT

100% Audit Pass Rate

First-Time Certification, Zero Major Non-Conformities

Achieved first-time ISO 27001:2022 accredited certification with zero major non-conformities and zero disruption to core product engineering.

THE CHALLENGE

DropStream, a high-growth SaaS platform automating fulfillment integrations across hundreds of shopping carts, marketplaces, and warehouse management systems, needed independent proof of institutional information security to win enterprise clients. As a lean, engineering-focused organization, the path to ISO 27001 certification felt opaque and overwhelming. They lacked the internal GRC expertise to navigate the standard's complex requirements and could not afford to divert their development team to build out compliance documentation from scratch.

WHAT WAS AT RISK

- Enterprise sales pipeline stalled by security review bottlenecks with 3PL and retail clients.
- No internal GRC expertise to interpret or implement the ISO 27001 standard.
- Risk of derailing core product engineering operations during certification build-out.

© 2026 Nexeris. All Rights Reserved.

THE SOLUTION

Nexeris designed and executed a hands-on, right-sized ISMS implementation tailored to DropStream's cloud-native architecture and agile operations.

RAPID MOBILIZATION

Rather than imposing a rigid framework, Nexeris mapped DropStream's existing AWS infrastructure, Ruby on Rails integrations, and engineering workflows directly to ISO 27001 controls to identify the most efficient path forward.

CO-DESIGNED CONTROLS

Nexeris co-designed right-sized policies and operational controls, including secure access management, encryption protocols, and vulnerability management that satisfied the 2022 standard without introducing unnecessary organizational friction.

MANDATORY INTERNAL AUDIT

Prior to the official registrar assessment, Nexeris conducted the mandatory internal audit, serving as a realistic dry run that isolated remaining process gaps and instilled the team with confidence.

FULL-LIFECYCLE AUDIT REPRESENTATION

Nexeris stood shoulder-to-shoulder with DropStream through both the Stage 1 (Documentation Review) and Stage 2 (Implementation Effectiveness) external certification audits, managing logistics and providing real-time support.

THE RESULTS

100%

Audit Pass Rate

First-Time Achievement

ISO 27001:2022 CERTIFICATION ACHIEVED

DropStream successfully achieved first-time ISO 27001:2022 accredited certification. The platform's security posture is now verified against all 93 Annex A controls, enterprise sales cycles are fast-tracked, and a lightweight continuous compliance program runs seamlessly alongside daily development.

- 100% first-time audit pass rate. Zero major non-conformities
- Enterprise risk questionnaires now fast-tracked, protecting pipeline revenue
- Security posture verified against all 93 Annex A controls by an accredited third party
- Sustainable, continuous compliance program embedded into daily operations

© 2026 Nexeris. All Rights Reserved.

"Nexeris was instrumental in guiding us through our ISO 27001 certification. Before our engagement, we genuinely didn't understand what the process involved — Nexeris took the time to really understand where we were as an organization first, then met us exactly where we were. They performed our initial internal audit and walked us through both the Stage 1 and Stage 2 audits all the way to certification. Throughout it all, they were always available to answer questions and work through any compliance challenge we encountered. I'd recommend them to any organization serious about building a resilient compliance program."

Karl Falconer
CTO, DropStream

DropStream

KEY TAKEAWAYS

MEET THE CLIENT WHERE THEY ARE

Effective GRC consulting does not mean forcing a small-to-midsize tech company to operate like a massive financial enterprise. Customizing policies to match existing operations accelerates implementation and ensures long-term operational success.

DEMYSTIFICATION DRIVES EXECUTION

High-stakes frameworks like ISO 27001 are intimidating to tech-focused teams. Translating compliance requirements into concrete, actionable steps removes internal paralysis and builds immediate momentum.

ACTIVE PARTNERSHIP VS. ADVISORY-ONLY

Guiding a client all the way through the final external audit, rather than simply handing over a gap assessment and walking away, guarantees a smooth certification process and creates an exceptional customer experience.

© 2026 Nexeris. All Rights Reserved.