Ropo

ISO/IEC 27001 Implementation

Ropo Group

12.8.2025
Kuopio, Finland

Introduction and Background

Ropo is the leading provider of invoice lifecycle services in the Nordics, with operations heavily based on digitalization, automation, and real-time reporting. Since Ropo handles large volumes of personal data from clients and end customers, information security is a core component of its business and customer trust.

To enhance information security management, Ropo has obtained the ISO/IEC 27001 certification for its Information Security Management System (ISMS), which is integrated into the company's broader management system. Ropo also holds ISO 9001 (quality), ISO 14001 (environment), and ISAE 3402 Type 2 report standards. ISO/IEC 27001 complements and unifies these frameworks, enabling a consistent and efficient governance model.

Practical Implementation and Governance Model

Ropo's Information Security Management System (ISMS) is designed to protect all critical business processes—such as invoicing, payment tracking, debt collection, customer service, and reporting—by following ISO/IEC 27001 standards. The system is built on a clear governance structure, robust risk management, documented policies, measurable objectives, and a cycle of continuous improvement.

Governance is centralized through a group-level Security Council, chaired by the CIO and including representatives from every operating country. This council ensures that information security initiatives align with corporate strategic goals. Risk management is integrated into this governance model: risks are systematically assessed, prioritized, and mapped to ISO/IEC 27001 control points, ensuring consistency across the organization.

To support this framework, a group-wide information security policy defines objectives, responsibilities, and guiding principles. This policy is mandatory for all employees and available in all operating languages, reinforcing a shared security culture.

Performance is monitored through defined metrics for each security objective. These metrics are regularly reviewed by the Security Council and the Group Management Team (GMT) to track progress and identify areas for improvement. Internal audits, conducted according to an annual plan, provide additional assurance. Findings from these audits feed into management reviews, driving corrective actions and ensuring the ISMS evolves to meet emerging risks and business needs.

Operational Execution of Information Security

Ropo's ISMS is embedded in day-to-day work, not just captured in documents. Every employee completes annual information security training, ensuring a shared baseline of awareness and role-specific responsibility. When incidents occur, they are handled through a centralized, predefined process that enables rapid response, consistent classification, and systematic learning—feeding improvements back into both training and controls.

Security extends beyond Ropo's boundaries through disciplined supplier management. All vendors must meet Ropo's information security requirements and sign data protection agreements before onboarding. Their practices are regularly audited, ensuring ongoing compliance and risk control across the supply chain. Transparent, timely communication—internally, with customers and partners, and externally through ESG reporting and ethical guidelines—reinforces accountability and trust.

Technical assurance underpins these practices. Routine vulnerability scanning and periodic penetration testing validate control effectiveness and identify weaknesses early. Collaboration with a Security Operations Center (SOC) provides continuous monitoring, threat detection, and incident support, improving response quality and reducing dwell time.

Change management ensures that modifications to systems and services are introduced safely. Changes are risk-assessed, tested, and approved before deployment, with performance monitoring in place to confirm stability and security post-release. Together with continuous security assessments, these activities create a closed loop: findings from monitoring, testing, audits, and incidents inform corrective actions and drive ongoing improvement across people, processes, and technology.

Data Protection and Personal Data Handling

Data protection is a core element of Ropo's ISMS, reflecting the critical importance of lawful and transparent handling of personal data. Given the significant volume of personal data processed, Ropo ensures full compliance with the EU General Data Protection Regulation (GDPR) and all applicable national laws.

A group-level Data Protection Policy sets out the principles, roles, and responsibilities for safeguarding personal data. Each operating country appoints a dedicated Data Protection Officer (DPO) to provide local guidance and oversight. These practices are fully integrated into the ISMS and are regularly monitored through internal audits and management reviews to ensure ongoing compliance and effectiveness.

Transparency is a key commitment. Customers can review Ropo's data protection practices through the privacy notice available on the company website (ropo.com). This notice clearly explains what data is

collected, the purposes of processing, and the legal basis for each activity. Additionally, an up-to-date list of data processors is published online, ensuring visibility and control across the entire service chain.

Business Continuity

Ropo's ISMS is designed to ensure uninterrupted operations, even under adverse conditions. Comprehensive contingency measures—including business continuity and disaster recovery plans—are in place to maintain critical services during disruptions such as cyberattacks, system failures, or other crises. These plans are fully documented, regularly tested, and updated to reflect evolving risks. This proactive approach guarantees service availability and secure data access for customers, reinforcing trust and resilience across all operations.

Competence

Ropo prioritizes building and maintaining strong security competence across the organization. All employees undergo regular information security training to ensure a consistent understanding of security principles and responsibilities. For those in security-related roles, deeper expertise in ISO/IEC 27001 requirements is expected and continuously developed through targeted training and professional development.

This commitment extends beyond internal teams. Suppliers and partners also receive security awareness training and must adhere to Ropo's security standards. By embedding competence throughout the entire service chain, Ropo ensures that customer data remains protected at every stage of the lifecycle, reinforcing trust and compliance across all operations.

Certification Benefits for Customers

Ropo's ISO/IEC 27001 certification provides customers with confidence that their data is managed securely and systematically. It confirms that security incidents are handled through defined processes and that all controls are documented, implemented, and regularly audited.

Beyond assurance, the ISMS supports customers in meeting their own regulatory obligations, including GDPR, NIS2, and DORA. Because the system is continuously improved and adapted to evolving risks and requirements, Ropo ensures that its services remain secure, compliant, and future-ready.