CASE STUDY

Implementing ISO 27001: Securing Information Across a Rapidly Expanding Logistics Network

Overview

i3Secure was engaged by a leading provider of chilled and ambient storage, transport, and packing services, with operations spanning across the UK, Ireland, and Europe.

Over several decades, the company has grown significantly through strategic acquisitions, including a number of renowned transport brands. This rapid expansion has led to the typical challenges of standardisation and efficiency across a diverse and growing business model.

With an increasing demand for secure management of customer data, financial records, and operational systems, the company recognised the importance of implementing the ISO 27001:2022 standard and establishing a robust Information Security Management System (ISMS) to safeguard their operations and ensure regulatory compliance.

i3Secure implemented an ISO 27001-compliant ISMS across the entire organisation, after previously delivering a successful implementation for one of their acquired companies.

The Challenge

The organisation faced several key challenges that are common in fast-growing organisations:

- **Data Protection and Regulatory Compliance:** As a large logistics and transportation provider, protecting sensitive customer and operational data was becoming increasingly critical, especially with their expansion into new markets.
- **Cybersecurity Threats:** The rapid growth led to a fragmented approach to information security, exposing the company to potential cyber risks, breaches, and compliance failures.
- **Operational Inefficiencies:** With multiple acquisitions, a lack of a standardised security framework made it difficult to implement consistent controls and processes across the business.

© 2025 i3Secure Ltd

Our Solution

To support rapid expansion and increasing data security demands, a leading logistics provider partnered with i3Secure to implement a robust ISO 27001-compliant Information Security Management System (ISMS).

Initial Assessment and Gap Analysis
We first comprehensively reviewed the organisation's security posture, identifying key vulnerabilities such as inconsistent IT design and undocumented procedures, laying the groundwork for a tailored ISMS.

Risk Assessment & Asset Identification
Critical operational data—like GPS tracking, shipment schedules, and customer information—were assessed for cyber threats and data loss risks, helping prioritise areas for immediate action.

Designing the ISMS Framework
Working with the internal security team, we developed a bespoke ISMS aligned with ISO 27001, defining clear policies, identifying key assets, and establishing incident response and disaster recovery plans.

Implementation of Controls
We introduced a suite of technical and organisational controls to protect sensitive data and minimise risks:

- Multi-factor authentication and secure access systems
- Regular vulnerability assessments and data backups
- Enhanced physical security and supplier diligence
- Secure staff movement protocols

Employee Training & Security Awareness
Recognising that a secure organisation begins with its people, we delivered targeted training across the organisation. This ensured staff at all levels understood their role in protecting information, embedding security awareness into the company culture.

Internal Audits and Corrective Actions
Internal audits identified further enhancements, such as improved visitor management and physical security protocols, ensuring continuous improvement.

Certification Preparation & Audit Support
We guided the organisation through audit readiness, resulting in a flawless Stage 1 Audit. During Stage 2, we provided on-site support, helping the client achieve certification on schedule, with no non-conformities.

The Result

The organisation successfully implemented ISO 27001, achieving the following key outcomes:

- **Enhanced Security Posture:** With the ISO 27001-certified ISMS in place, the organisation now has a robust system to safeguard critical data, significantly reducing the risks associated with cyberattacks and data breaches.
- **Regulatory Compliance:** The company is now fully compliant with global data protection standards, making them well-positioned to expand into new markets and enhance their reputation with clients and stakeholders.
- **Improved Employee Culture:** Security awareness and responsibility have been instilled across the workforce, with employees better equipped to handle security threats and follow best practices.
- **Operational Efficiency:** The implementation of ISO 27001 has streamlined security operations, reduced downtime caused by incidents, and enhanced incident response times, resulting in improved business continuity.

This project exemplifies how businesses in dynamic sectors like logistics can protect sensitive information, meet regulatory requirements, and enhance their overall operations.

i3Secure is ready to support your organisation in achieving these same results, ensuring a secure, compliant, and efficient future.

© 2025 i3Secure Ltd