SysGroup

CASE STUDY

UK-based Rail Firm

Introduction 01

Company Overview

SysGroup is a trusted provider of penetration testing, cyber maturity assessments, and compliance solutions. We empower organizations to secure their infrastructure, reduce risk exposure, and build long-term cyber resilience.

Client Background

Our Client operates within the UK rail sector, supporting critical national infrastructure. With a growing need to meet industry regulations and demonstrate robust cybersecurity practices, The Client engaged SysGroup to assess its cyber maturity and establish a roadmap towards internationally recognized standards such as ISO 27001.

Challenges 02

Initial Situation

For an organization of its size, our Client was assessed as having a low level of cyber maturity, below the industry average. Key gaps existed across security governance, access control, asset management, and incident response. Additionally, there was no formal ISO 27001 implementation project in place, leaving the organization exposed to risks and limiting its ability to meet compliance and client expectations.

Objectives

- Identify and remediate security weaknesses across people, processes, and technology.
- Provide a clear, prioritized action plan to raise cyber maturity.
- Develop a roadmap for ISO 27001 certification to support regulatory compliance, client confidence, and new business opportunities.

© 2025 SysGroup

Solution 03

Approach

SysGroup conducted a comprehensive **Cyber Maturity Assessment (CMA)** against ISO/IEC 27001:2013. The process included workshops, stakeholder interviews, technical vulnerability assessments, and a review of policies, procedures, and physical security. Findings were mapped against ISO 27001 requirements, ISO security controls, and NCSC's Cyber Assessment Framework.

Implementation

- Developed a detailed action plan with 76 prioritized actions (51 high, 18 medium, 7 low).
- Proposed a 14-week remediation programme combining policy updates, technical measures, and governance improvements (e.g., clear security roles, access control enforcement, cryptography policies, supplier risk management).
- Created an ISO 27001 certification roadmap covering ISMS build, leadership commitment, risk management, ISMS operation, performance evaluation, and external audits.
- Provided delivery model options ranging from full SysGroup-led implementation to client-led delivery with expert review.

Results 04

Outcomes

- Delivered a transparent maturity assessment with clear evidence of deficiencies.
- Provided a structured remediation and certification roadmap, tailored to the Client's resources and strategic priorities.
- Enabled our Client to make an informed decision between simply remediating vulnerabilities or pursuing ISO 27001 certification.

Benefits

- A practical, prioritized action plan for closing cyber gaps quickly.
- A sustainable framework aligned with ISO 27001, ensuring long-term compliance and scalability.
- Clear alignment with NIS Directive requirements and wider industry standards, strengthening the Client's position in the sector.
- Support for business growth, as ISO certification improves credibility with partners, regulators, and customers.

Conclusion 05

Summary

SysGroup successfully assessed our Rail Client's cybersecurity maturity, provided a detailed remediation plan, and designed a roadmap to ISO 27001 certification. This ensured Rail Client could move from low maturity towards a resilient, standards-aligned security posture.

Future Plans

The Client is now considering **ISO 27001 certification** as the recommended option, enabling long-term security, compliance, and competitive advantage. SysGroup stands ready to support with continued advisory, technical expertise, and certification preparation.

© 2025 SysGroup