Impact Compliance Solutions

Case Study

ISO/IEC 27001 Implementation

Introduction

Impact's Head of Compliance has led multiple implementations of the ISO/IEC 27001 Information Security Management System (ISMS). This case study outlines a project involving a UK-based technology company specialising in immersive digital platforms and virtual collaboration tools.

The Client

The organisation operates in a fairly complex space, combining cloud infrastructure, real-time user interaction, and user-generated content. From a security perspective, that creates a different set of challenges compared to more traditional environments. We needed to take what was already a technically capable business and formalise its approach to information security in a way that aligned with ISO 27001, while still working in practice. The driver behind the project was the need to strengthen security maturity, protect sensitive data, and meet increasing expectations from enterprise clients.

Project Overview

Objectives

The objective was not simply to obtain certification but to create a sustainable security framework. The organisation needed to protect key assets, including platform data, client environments, and internal systems, while supporting business growth. Certification also offered a recognised way to demonstrate security credibility to clients. Another goal was to increase internal awareness and embed information security within daily operations.

Scope Definition

Defining the ISMS scope was an important early step. Working with leadership, the scope was set to include the platform's development and operation, cloud infrastructure, internal business systems, and remote working environments. Third-party services supporting the platform were also considered within the risk management process.

Gap Analysis and Planning

A gap analysis against ISO/IEC 27001 revealed that while the organisation had strong technical capabilities, formal security management processes were limited. Key gaps included risk management, documentation, and consistency in applying security practices. Incident management and supplier assurance processes also required improvement. Based on these findings, an implementation roadmap was developed to prioritise high-risk areas while remaining realistic in terms of resources and timelines.

Key Points

- **One challenge was applying ISO 27001 to a non-traditional technology environment** where some requirements required interpretation.
- **Balancing strong security controls** with operational usability was also important.
- **Controls needed to be effective** without creating unnecessary complexity.
- **Communication and engagement** across the organisation are as important as the technical controls themselves.

We're proud to be a BSI Member

The Board of The British Standards Institution is committed to the highest standards of corporate governance which it considers fundamental to business's success.

bsi Membership
February 2026—January 2027

Risk Assessment and Treatment
A structured risk assessment process was introduced to identify assets, evaluate threats, and assess risks using a consistent scoring approach. Given the nature of the platform, risks included unauthorised access to client environments, handling of user-generated content, and vulnerabilities related to real-time communication features. Risk treatment plans were developed using ISO 27001 Annex A controls as a reference. A risk register was established and maintained as a central and regularly updated part of the ISMS.

ISMS Development and Control Implementation
Core ISMS documentation was developed with a focus on clarity and practicality. Key policies included the Information Security Policy, access control, acceptable use, incident management, and data handling. Technical improvements were implemented in collaboration with engineering teams. These included enhanced access management, multi-factor authentication, consistent encryption practices, and improved logging and monitoring. Supplier management processes were also formalised to address third-party security risks.

Awareness and Cultural Integration
Ensuring organisational engagement was essential. Role-based security training was introduced to make guidance relevant to different staff groups, including developers and non-technical employees. Security processes were integrated into existing workflows, particularly within development processes, to ensure adoption without disrupting productivity.

Internal Audit and Management Engagement
An internal audit programme was established to assess the effectiveness of the ISMS and identify areas for improvement. Regular management review meetings ensured senior leadership maintained visibility of security risks, audit findings, and ISMS performance, helping drive organisational commitment.

Certification Process
The organisation was prepared for the ISO 27001 certification process, including both Stage 1 and Stage 2 audits.

- **Stage 1** focused on documentation and readiness.
- **Stage 2** assessed how effectively the ISMS operated in practice.

Due to prior internal audits and preparation, the external audit process was smooth, and the organisation successfully achieved ISO/IEC 27001 certification.

Outcomes and Benefits

Following implementation, the organisation **gained a structured approach** to information security. Risks were better understood, controls were applied more consistently, and **visibility across systems improved**.

Certification **strengthened client trust and supported new business opportunities**, while internally **providing a stronger foundation** for ongoing security management.

Conclusion

This project demonstrated that **ISO/IEC 27001 can provide significant value when implemented in a practical and proportionate way**. By aligning the ISMS with real operational processes, the organisation achieved both certification and meaningful improvements to its security posture.

The result was a more resilient organisation with information security embedded into everyday operations.