Impact Technology Solutions

Case Study

ISO/IEC 27001 Implementation

UK Based Digital Infrastructure & Managed Platforms Provider

Introduction

This case study outlines the implementation of an ISO/IEC 27001 Information Security Management System (ISMS) for a UK based organisation delivering secure digital infrastructure, managed platforms, and business critical hosted services. The engagement focused on establishing proportionate and auditable information security governance while supporting a fast paced, service led operating model.

The Client

The organisation provides managed digital services to commercial and public-sector clients, including hosted platforms, secure connectivity, and ongoing technical support. Due to the nature of its services, the organisation processes sensitive customer information and operates systems that are critical to client operations. While robust technical controls were in place, the organisation required a structured and formally governed ISMS to meet increasing client expectations and contractual information security requirements.

Project Overview

Objectives

The primary objective was to implement an ISO/IEC 27001-aligned ISMS that was practical, effective, and embedded within existing operational processes. Certification was sought to provide independent assurance of information security management, strengthen client confidence, and support future business growth. A further objective was to establish clear senior management ownership of information security risk.

Scope Definition

The ISMS scope included the delivery and support of managed digital services, internal business systems, cloud hosted infrastructure, and remote working arrangements. Third party suppliers supporting service delivery were incorporated into the risk assessment and supplier management processes to ensure appropriate end to end security oversight.

Gap Analysis and Planning

An initial gap analysis against ISO/IEC 27001 identified that, although technical security measures were well developed, formal risk management processes, documented controls, and consistency of application required improvement. Identified gaps included supplier assurance, incident management, and demonstrable governance. A structured implementation plan was developed to address higher risk areas as a priority, aligned to available resources and operational capacity.

Key Considerations

- Applying ISO/IEC 27001 within a managed services environment required proportionate interpretation to **ensure controls were effective and operationally appropriate**.
- Information security controls needed to **support service availability and responsiveness** rather than impede service delivery.
- **Effective communication between technical teams and senior management** was critical to successful implementation.

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 methodology was introduced to identify information assets, assess threats and vulnerabilities, and evaluate risks using a consistent approach. Risk treatment plans were developed with reference to ISO/IEC 27001 Annex A, and a central risk register was established and maintained as a core element of the ISMS

ISMS Development and Control Implementation
Core ISMS documentation was developed, including the Information Security Policy and supporting procedures for access control, incident management, supplier management, and information handling. Existing technical controls were reviewed and enhanced where appropriate, with emphasis on access management, monitoring, and secure configuration. Supplier assessment and assurance processes were formalised to address third-party information security risks.

Awareness and Cultural Integration
Role appropriate information security awareness training was implemented to ensure staff understood their responsibilities. ISMS processes were aligned with existing operational workflows to promote adoption and minimise disruption to day to day service delivery.

Internal Audit and Management Engagement
An internal audit programme was established to evaluate ISMS effectiveness and identify opportunities for improvement. Management review meetings provided ongoing oversight of information security risks, incidents, audit outcomes, and ISMS performance, reinforcing leadership commitment and accountability.

Certification Process
The organisation was prepared for both Stage 1 and Stage 2 ISO/IEC 27001 certification audits. Due to structured preparation and internal assurance activities, the external audit process was completed efficiently, resulting in successful certification.

Outcomes and Benefits
The organisation achieved a consistent, structured, and auditable approach to information security management. Certification strengthened client confidence, supported contractual and assurance requirements, and provided a robust framework for ongoing information security risk management.

Conclusion
This project demonstrated that ISO/IEC 27001 can be implemented in a practical and business-aligned manner within a managed services environment. The outcome was a more resilient organisation with information security embedded into normal business operations.