

The Business Drivers behind Compliance



Esteem specialises in delivering a full and comprehensive range of IT services that are designed to care for the entire lifecycle of an IT infrastructure including consultancy, design, implementation and on-going management. Esteem works with clients across the private and public sectors including Scania (Great Britain), the Nottinghamshire Building Society, Avon and Wiltshire Mental Health Partnership NHS Trust, University of Salford and BT.

Esteem's vision for the future is clear: to be a total lifecycle services provider, delivering a full range of managed services that complements its business solutions and enhances the services it offers to its customers, protecting their IT infrastructure investments.

Esteem recognised that achieving compliance to ISO27001 would provide reassurance to their existing managed service customers and potential future customers. They considered compliance to ISO27001 to be beneficial in ensuring that the confidentiality, integrity and availability of its organisational information assets was maintained at the highest levels. This, in turn would enable Esteem to ensure a high level of service to its customers.

Finding the Right Partner

Esteem chose independent security advisor Sapphire to help achieve compliance. Sapphire has been providing information assurance consultancy for over a decade. Esteem chose Sapphire for many reasons; in particular Sapphire provided realistic timescales for implementing the management system to compliance level, taking only 19 days across 5 key phases:

- **Phase 1** - Diagnostics: Current State Analysis / Risk Management
- **Phase 2** - Security Improvement Plan
- **Phase 3** - Security Awareness Education and Training
- **Phase 4** - Implementation Review and Compliance Checks
- **Phase 5** - Discussion and Development of Next Steps

Esteem already adhered to strict procedures, but they did not have written policies in place for these procedures to integrate with the standard.

Andrew Parry was the consultant assigned to this project. Andrew has over four years experience in leading organisations to both ISO27001 compliance and certification. Throughout, Andrew assisted Esteem with the development of all documentation required for compliance.



“Finding the right consultant was an important part of the project. Changing culture within an organisation and encouraging staff to embrace that culture can be difficult. Sapphire’s consultant, Andrew, worked with us to make this change. He knew the subject matter and was always helpful when we had any queries, or a change of focus. The staff at Sapphire went out of their way to understand our organisation and the individuals within it. Sapphire’s process worked for us.”

Tim Loughlin, Chief Finance Officer, Esteem

Together, Andrew and the ISO team at Esteem educated staff in a series of workshop sessions spread across 3 days with additional training sessions being provided to the Professional Services Department. Internal Audit training was also delivered through half day courses which are in line with ISO 19011 (the international standard for audit) to nominated individuals.

Achieving Compliance

The compliance project was completed within the defined timescale. Esteem’s existing customers now have a documented assurance that Esteem take security seriously by operating a formal Information Security Management System (ISMS).

Compliance allowed Esteem to achieve all of its goals including:

1. Achieving a higher level of business resilience by operating ISMS which in turn provided added assurance to its existing client base.
2. Being able to demonstrate that client data is firmly managed and secured when held by Esteem.
3. Compliance to ISO27001 enabled Esteem to tender for new contracts where compliance was a pre-requisite
4. Esteem now has a fully compliant, operational management system and has implemented controls which manage identified threats and vulnerabilities and operates a cycle of continual improvement throughout the organisation.

Esteem is now in the process of achieving formal certification to the standard.

