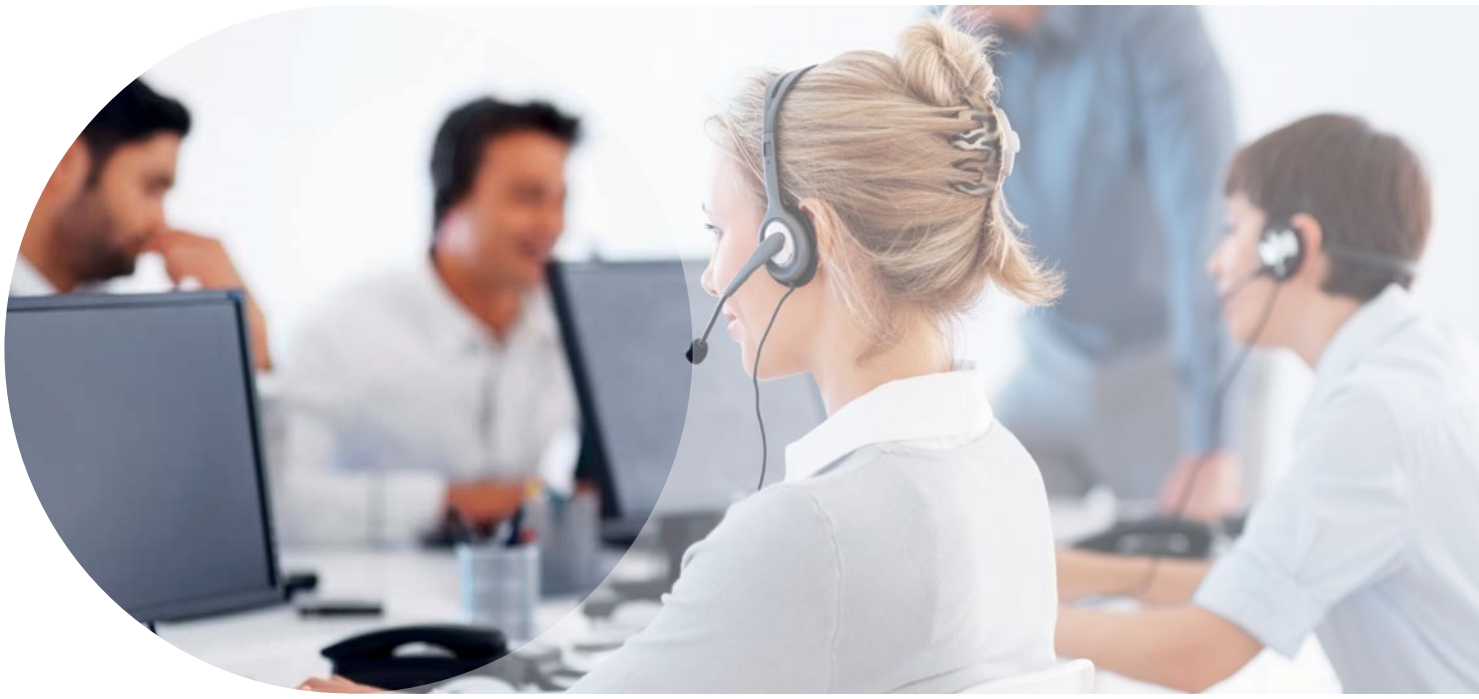

Implementing best practice and improving client confidence with ISO/IEC 27001

"We aspire to provide our clients with the best possible service to the highest standards. Our ISO/IEC 27001 certification with BSI allows us to provide our clients with confidence that their information is being protected in accordance with an internationally recognized security standard."

Ian Waterhouse
Information Security Programme Manager,
Legal Ombudsman for England and Wales

Customer needs

- Greater information security awareness
- To demonstrate due diligence and compliance in handling sensitive information
- An assurance framework aligned with global best practice

Customer benefits

- Improved client confidence and reassurance
- Improved security and a reduction in risk through better understanding
- Process improvements across the organization
- Enhanced reputation and brand

Customer background

The office of the Legal Ombudsman for England and Wales was set up by the Office for Legal Complaints under the Legal Services Act 2007 in an attempt to simplify the system and ensure consumers had access to an independent expert to resolve complaints.

The Legal Ombudsman is based in Birmingham and its service is open to all members of the public, very small businesses, charities, clubs and trusts. Its 300 staff receive some 1,500 contacts each week and handle 8,420 cases per annum. Its task is to run an independent ombudsman scheme that resolves complaints about lawyers in a fair and effective way with the aim of driving improvements in the provision of legal services.

Part of the challenge for the Legal Ombudsman, as well as the regulator, is to try to anticipate changes to the market and ensure that it is ready to respond. In a market such as legal services, which is changing so rapidly, that is not an easy task.

Why certification?

The Legal Ombudsman takes customer service very seriously and is committed to providing its clients with the best possible service and to the highest standards. Protecting its clients' privacy and ensuring the confidentiality of their records is a critical aspect of this, and it wanted to provide its clients with the assurance that their information is being protected in accordance with an internationally recognized security standard.

Benefits

Obtaining certification to ISO/IEC 27001 has provided a level of confidence to users of the Legal Ombudsman's services that their personal data is secure.

The initial risk assessments that the Legal Ombudsman carried out as part of its implementation of the management system have ensured that risks to the organization's information are now understood at a much more granular level and are being properly managed.

The process of implementing ISO/IEC 27001 has strengthened the Legal Ombudsman's internal organization. Improvements have been seen across the business but most notably in areas not directly within IT. Achieving buy-in has been an important part of its success, resulting in improved awareness across the organization and a willingness to address poor practices.

The Legal Ombudsman's implementation of ISO/IEC 27001 has also brought about improvements in its brand reputation. Its certification to the global standard is displayed proudly on its website and within documentation resulting in improved client confidence that information they pass on will be securely handled.

Implementation

The Legal Ombudsman worked with information security consultancy Aristi Limited on the implementation of its ISO/IEC 27001 information security management system (ISMS). Having worked with them previously, in relation to the HMG Accreditation Programme, Aristi already had a good understanding of the business and its processes, making the decision straightforward.

Having undertaken a gap analysis, the Legal Ombudsman was pleased to discover that it already had approximately 75 percent of the system requirements in place as a result of the work done during the HMG Accreditation process. However some adjustments were required to meet the differing requirements of the ISO/IEC 27001 standard.

The Legal Ombudsman went about implementing ISO/IEC 27001 by first developing a project plan. It engaged with BSI early on and worked with Aristi and BSI to define an appropriate scope for the ISMS, which took into account key assets and business processes. This formed the basis of the subsequent compliance implementation activities.

The Legal Ombudsman reviewed its existing asset list and risk assessment methodology and used this to conduct a risk assessment against the ISMS scope. This allowed the appropriate management action and priorities for managing information security risks to be determined. Existing security policy documents were reviewed and updated to meet the requirements of ISO/IEC 27001 and work was undertaken to implement the policies. Adequate and proportionate security controls such as policies, procedures and technical functions were put in place, and a security awareness programme was developed to embed this thinking into its employees everyday working practices and bring about a 'security culture' within the organization.

Once the system had been successfully implemented, the Legal Ombudsman underwent a gap analysis, after which they addressed the last of the issues. At this point BSI conducted a formal independent third party audit of the new ISMS.

Staff awareness training was vital to the success of its implementation project. As part of the process, all employees completed awareness training and its various business units were given responsibility for ensuring the requirements were embedded into the organization's business process.

Data owners were engaged in the Business Impact Assessments to ensure that information assets were appropriately valued and departmental champions were selected to ensure that standards are adhered to and maintained in each of the business units.

Having already completed its HMG Accreditation, the Legal Ombudsman had a good idea of what to expect and found the development process relatively straight forward.

The most difficult aspect of the implementation project was the process of carrying out the risk assessments, an aspect it had never done before to the level and detail required for ISO/IEC 27001. This was overcome by taking advice from its consultant who helped produce a detailed matrix of risks and mitigations.

The programme took eight months to implement and was led by Ian Waterhouse as Programme Manager, Paul Connor as Technical Lead and supported by the Executive Management Team.

BSI's role

The Legal Ombudsman decided to work with BSI on the recommendation of its consultants. As authors of the original standard for information security (BS 7799) it was felt that BSI was best positioned to provide certification. The BSI Client Manager carried out both the stage 1 and 2 audits of the system and will continue to visit over the next three years to carry out continuing assessment audits to ensure ongoing compliance and help with continual improvements.

"The ongoing relationship and certification with BSI gives us piece of mind that the system will remain current and relevant, helping us maintain excellent information security management" explained Ian Waterhouse, Information Security Programme Manager.

bsi. ISO/IEC 27001 Information Security Management

bsi.

+44 845 080 9000
certification.sales@bsigroup.com
bsigroup.com