Bevan Brittan
The public services law firm

BACKGROUND

Bevan Brittan is the largest specialist provider of public services legal advice in the UK. Its clients include NHS trusts, local authorities, housing associations and over 100 private sector firms which serve the public services market. The Firm operates throughout the UK with offices in London, Birmingham and Bristol. Bevan Brittan was formed by the demerger of Bevan Ashford in 2004 and can trace its roots back to 1815.

Reflecting the demands and requirements of the public services market sector which the Firm operates in, Bevan Brittan prides itself on its mature management, systematic working practices and an inherent appreciation and awareness of the importance of information security. Peter Rogers, Director of Risk at Bevan Brittan, believes that "With its history of dealing with public sector organisations and top down commitment, the Firm has developed a very mature governance structure with a strong and unified culture across all of its 3 sites."

In November 2013, Bevan Brittan secured certification to ISO 27001, the International Standard for Information Security Management. This case study highlights some of Bevan Brittan's key experiences, business drivers, success criteria and benefits derived.

Business Drivers

Bevan Brittan identified the clear benefits attached to certifying to ISO 27001, as Keith Lyall, Risk & Best Practice Manager, explains "Bevan Brittan has always understood the importance of protecting client data. With ISO 27001, however, there is the external validation that certification brings, as well as the practical benefits when completing tenders and questionnaires which specifically refer to ISO 27001 certification. Clients tell us that they want to be sure that the work that we do is consistent, concise, secure and commercial. They also tell us that they want the systems, processes, procedures and working practices that support our service delivery to be externally validated. Having certified to the ISO 9001 Quality Management System, we had already established strong processes and management systems. This provided a solid foundation on which we could build on to comply with ISO 27001."

There was an appreciation that the exercise would be expensive, both in terms of money and also internal manpower. Whilst these impacts could not be ignored in what was a challenging economic climate, Bevan Brittan's Board believed that the potential/perceived long term benefits would outweigh the short term pain and costs. The three key business drivers identified were:

- Further tightening of information security practices and controls, reducing the likelihood of a security breach and the potential damage to the Firm's reputation and brand
- Providing Bevan Brittan with a competitive advantage, particularly in a bidding situation, facilitating revenue generation
- Enabling Bevan Brittan to save time and money when completing questionnaires and tenders. Those organisations which are not certified to ISO 27001 typically have to spend longer completing such documents, and sometimes have to provide more information about policies, procedures and working practices.

KEY STAGES

Selection of Key Partners

Whilst Bevan Brittan held a natural and healthy suspicion of consultancy organisations, it acknowledged that it could benefit from the support of a specialist consultancy to assist in meeting specific requirements of the Standard.
Of particular concern was how to conduct an information security risk assessment and validate that technical controls adopted were appropriately implemented. URM was selected due to its:

- Ability to tailor its support approach
- Willingness to maximise use of existing policies and practices to ensure the resulting ISMS fitted Bevan Brittan's culture
- Risk expertise and assessment tool
- Depth of consultancy team i.e. not a one man band
- Track record in supporting legal practices; URM was recommended by another Firm

Whilst certified to ISO 9001 with another organisation, British Standards Institution (BSI) was selected as the ISO 27001 certification body on the basis of the depth and calibre of its ISO 27001 assessors.

Scope

It was accepted that the easiest approach would have been to certify one of its sites and then to roll out its ISMS across the other offices. However, it was decided to seek certification across the whole organisation and all sites i.e. Bristol, Birmingham and London. This decision was heavily influenced by the fact that:

- A number of key clients access services from across all three of Bevan Brittan's offices
- There is a high degree of overlap/replication of services between sites and the Firm enjoys a consistency of infrastructure and culture
- There is significant movement of staff between sites and it is important that there is a consistency of working practices between offices e.g. Clear Screen Policy.

Risk Assessment

Bevan Brittan was implicitly familiar with the concept of risk management having conducted numerous high level risk assessments and established a strategic risk register, but the Firm had never conducted a detailed information security risk assessment.

The information risk assessment report acted as the catalyst for change and led to a clear, prioritised programme of control improvement work for Bevan Brittan to complete before certification could be achieved. The combination of URM's consultants and the adoption of URM's Abriska risk assessment software gave Bevan Brittan confidence that the resulting risk assessment would fully address the requirements of ISO 27001.

Policy, Process and Management System Development

The importance of good information security practice is well understood within Bevan Brittan. Client confidentiality is a fundamental principle of the solicitor-client relationship in England & Wales and the need to safeguard client information has been at the heart of the firm's approach since it's foundation in 1815. At the same time, it was absolutely critical that Bevan Brittan was not burdened with a cumbersome information security management system (ISMS) and an overload of inappropriate and unnecessary policies and processes. Bevan Brittan's objective was to establish a minimal number of 'shall do' documents, with a preference to issue advisory and guidance documents. As a result, Bevan Brittan, with guidance from URM, produced a small set of essential policies including 'Acceptable Use', 'Encryption' and 'Remote Working'. In addition, wherever possible, Bevan Brittan integrated the requirements of the ISMS into its existing management system activities.

Awareness Training

Communication of the importance of information security was seen as a key requirement, particularly for support services staff. It was identified that this group of staff naturally had a lower intrinsic awareness of the importance of information security compared to the lawyers. To address this requirement, all staff (directly or indirectly employed) undertook an online information security training session in addition to the existing online Data Protection training. This session had been developed to communicate key information security principles and Bevan Brittan's expectation of compliance with established policies and processes. Staff needed to complete and pass a test to demonstrate an understanding across all areas.

URM's consultant was adept in understanding Bevan Brittan and tailoring her approach appropriately.

Keith Lyall

KEY SUCCESS CRITERIA

A key success criteria of the ISO 27001 certification project was the full integration of any outputs with existing practices and the organisation culture. At every opportunity, Bevan Brittan's approach was to understand the objectives of the Standard and, where possible, maximise the use of what (policy, process or practice) was already in place.

Minimise Policies and Adopt Cultural Approach of Guidance Documents

Keith Lyall strongly believes "The culture of Bevan Brittan is such that prescriptive policies, applied across the organisation would inevitably be questioned and challenged as to their appropriateness. Wherever possible, an approach built on providing guidance documents based on best practice principles was adopted with local interpretation being left to individual Practice areas."

Strong Foundation i.e. Good Physical Access

In addition to having a strong culture with regards to safeguarding information, Bevan Brittan had equally established strong controls with regards to the physical security of its offices. Blessed with similar infrastructures across all three sites, the Firm was able to apply access controls consistently across all offices.

Senior Sponsor and Strong Compliance Team

Bevan Brittan's implementation of an ISO 27001 certifiable ISMS was simplified by the fact that it was sponsored by the Director of Risk, a Board level appointment, and also by a compliance team already familiar with the requirements of an ISO management system.

Consultancy

The role of the URM consultant was key in leading the risk assessment phase and ensuring all of the risk reports and other documentation required by the Standard were produced. At the same time, the consultant demonstrated a flexible and 'light touch' approach when reviewing areas where the Firm had established working practices. Keith Lyall describes how "URM's consultant was adept in understanding Bevan Brittan and tailoring her approach appropriately." This method of work was invaluable, both during the Firm's implementation of ISO 27001 and during the certification assessments.

Abriska

Having engaged URM to conduct the initial information risk assessments using Abriska, URM's purpose designed risk assessment tool, Bevan Brittan recognised the benefits of adopting the product to support the ongoing maintenance and development of its risk assessments. Keith Lyall explains "Getting to grips with the risk assessment requirements of the Standard and the functionality of Abriska was greatly enhanced by the fact that we were able to adopt the tool pre-populated by URM with our risk assessment data. Abriska produces the key reports required by ISO 27001 including a statement of applicability (SoA), risk matrices and risk treatment plan and it is difficult to see how these can be simply and easily produced and maintained without the use of such a tool."

BENEFITS SEEN

Added Rigour to Working Practices

Having a structured style to managing its approach to information security has added more rigour in the application of some of the related controls e.g. access control, IT controls, starters and leavers processes. The ISO 27001 Standard has also prompted Bevan Brittan to implement processes to ensure evidence is available which demonstrates that its ISMS is operating effectively.

Practice Wide Benefits

Whilst achieving certification to ISO 9001 was an important step for Bevan Brittan, Keith Lyall believes "the impact and benefit of achieving ISO 27001 certification was more far-reaching and touched all areas, including support functions such as HR, IT and Finance. Implementing ISO 27001 proved to be a useful tool in initiating change throughout Bevan Brittan and has undoubtedly generated improvements in policy, process and practice across the Firm."

Client Reassurances

A key driver for securing ISO 27001 certification was to allow Bevan Brittan to provide reassurance to its clients that a 'best practice' approach to information security was adopted within the Firm. Having secured certification to ISO 27001, Bevan Brittan is subject to continuous assessment visits by BSI, its chosen certification body. By maintaining its certification, Bevan Brittan is able to demonstrate its approach to information security management is not only being maintained, but is also being continuously improved.

More Effective Supplier Management

Establishing an ISO 27001 certifiable ISMS has not only clarified what information security arrangements Bevan Brittan needs to implement to meet its own operational requirements, but it has also clarified the security related expectations of services provided by key suppliers e.g. with regards to IT and administration arrangements.

NEXT STEPS

Bevan Brittan actively promotes its certification to ISO 27001 on its website and anticipates that demonstration of certification to this Standard will further reinforce existing client relationships and support its efforts in tendering for future business. Having secured certification to the Standard, the main challenge is to ensure that the ISMS is maintained and developed in a way that continues to address the requirement of the Standard as it evolves and equally drives real operational and commercial benefits for the Firm.

Bevan Brittan
The public services law firm

For more information on Bevan Brittan's legal services:
T: 0870 194 1000
E: info@bevanbrittan.com
W: bevanbrittan.com

URM

For more information on URM's consultancy services:
T: 0118 2065 410
E: info@urmconsulting.com
W: www.urmconsulting.com

bsi.

For more information on certification to ISO 27001 with BSI:
T: 0845 080 9000
W: bsigroup.co.uk/infosec