BACKGROUND

BLM is a long established legal practice which can trace its origins back to the 18th century. As a Top 50 law firm, BLM encompasses 170 partners, 700 lawyers and a total of 1,550 staff located in offices in Birmingham, Bristol, Cardiff, Dublin, Edinburgh, Glasgow, Leeds, Liverpool, London, Manchester and Southampton.

The Firm operates in eleven markets: brokers; construction & property; general insurance; healthcare; leisure & hospitality; Lloyds & London market; manufacturing; public sector; retail; TMT; transportation & logistics. A distinctive area of competence is its specialism in providing dispute resolution services to the insurance industry, where it manages in excess of 40,000 instructions per annum.

BLM's success has been achieved by building long term and strategic partnerships with its clients, where it has adapted its service delivery, communications and availability to meet individual customer requirements. Underpinning its service delivery are tailored service level agreements backed by Lexcel accredited case handling and an ISO 9001 certified quality management system, which provides relevant key performance indicators and mechanisms to drive continuous improvement.

As a major supplier of dispute resolution services, BLM manages significant volumes of sensitive and personal information on behalf of its insurance clients. As such, the Firm needs to demonstrate that it adopts a 'best practice' approach to information security management. With this requirement in mind, BLM identified securing certification to ISO 27001, the International Standard for Information Security Management, as the means for both achieving and demonstrating a 'best practice' information security approach. This case study shares some of BLM's experiences, including business drivers, implementation stages and benefits derived.

ISO 27001 BUSINESS DRIVERS

As a strategic partner, BLM undertakes regular reviews of its service delivery arrangements with its key clients. A key element of these reviews is the approach to information security that BLM has established to meet each client's specific requirements. It was clear to BLM that many of its clients' information security requirements were common and could be satisfied by the Firm aligning and certifying to ISO 27001. Achieving certification was seen as an ideal way of formalising BLM's existing information security approach and establishing an ongoing programme of continuous improvement.

KEY STAGES OF ISMS IMPLEMENTATION

Selection of Key Partners

One of BLM's first steps in attempting to secure ISO 27001 certification was to identify a consultancy partner who could assist it in both establishing a management system which would meet the requirements of the Standard, as well as being sympathetic to the culture and existing working practices of the Firm. BLM invited URM to submit a proposal for this support and believed the latter's client-centric approach, together with its broad ISO 27001 implementation experience, would provide the optimum level of support required. Equally, the skills transfer, training and software solutions offered by URM would ensure the ongoing development and maintenance of its information security management system (ISMS) could be increasingly brought in house.

BLM selected the British Standards Institution (BSI) as its certification body because achieving a certificate issued by BSI would have the greatest market recognition.

Development of Policies and Processes

Prior to targeting certification to ISO 27001, BLM had implemented a range of policies, processes and working practices to safeguard the information used to support its service delivery. Following a series of reviews of its information security approach (both internal and client driven), a number of improvement areas were identified. BLM's initial focus was to address these areas before embarking on a programme of works to establish an ISO 27001 certifiable ISMS. This ongoing effort has involved establishing a robust and repeatable risk assessment methodology, policy development, establishing BLM's information security forum (ISF) and undertaking regular management review.

Jonathan Clay, Partner - Manchester, states: "BLM needed to adopt a pragmatic approach that addressed the immediate concerns of any client around information security. However, BLM also wished to establish an ISMS that would ensure that a 'best practice' approach to information security was maintained and any ongoing changes required to BLM's current information security policies, processes and practice were managed in a controlled and appropriate manner."

> *"BLM needed to adopt a pragmatic approach that addressed the immediate concerns of any client around information security."*
>
> Jonathan Clay, Senior Partner - Manchester

Scope of Certification

BLM identified that targeting the whole organisation for certification would be challenging, but was concerned that any scope must be meaningful and add value from a client perspective. As such, the Firm decided to focus its initial certification scope on protecting the data associated with the service delivery conducted at its Manchester and London offices. These offices provide key services (HR, IT, Finance etc.) to the Firm and support the delivery of key legal practice areas. BLM was confident that as it developed its ISMS against this initial scope, it would be relatively straightforward to extend the scope to its other offices. BLM briefly considered focusing the scope against its IT service provision, but as Neil Brenner, the Firm's Information Security Officer explains "We quickly identified that a broader scope (including legal practice areas), was better. Whilst potentially more challenging, this would be more credible in demonstrating our commitment to fully addressing all aspects of information security related to our service delivery."

Internal Communication

Prior to seeking certification, BLM embarked on a comprehensive training and awareness programme to support the implementation of developed policies, procedures and activities and to ensure that information security 'best practice' was fully embedded within all London and Manchester practice and support areas.

Certification Assessment

Having established an ISO 27001 certifiable ISMS, BLM was determined that the resulting certification carried as much weight as possible. Having considered the options available, BLM decided to engage the BSI to conduct the assessment activity associated with securing and maintaining formal certification to this Standard. BLM's assessment was that achieving certification with the BSI would be a 'benchmark achievement' which would be recognised and appreciated by its clients.

KEY SUCCESS CRITERIA

Senior Management Commitment

The support and participation of BLM's Senior Management was absolutely key to the Firm securing certification to ISO 27001. The support was critical in ensuring the project was appropriately resourced and there was an ongoing commitment to management reviews and the updating of policies and practices. The involvement of 'project sponsor' Jonathan Clay, Senior Partner - Manchester, was central to ensuring the project received the support of partners and staff alike.

Training and Awareness Programme

As part of its ISMS implementation, BLM embarked on an extensive awareness programme which included short presentations to all staff, supported by a range of posters and a dedicated information security area on BLM's intranet. This has significantly raised the profile of information security within the Firm and has encouraged staff to submit ideas for improving information security management.

Consultancy / Skills Transfer Support

Over a period of time, URM worked closely with BLM to provide knowledge and support in developing its information security response and developing its ISMS. URM consultants also played a useful role by attending the formal certification Stage 1 and Stage 2 assessments, helping to ensure the external assessor's requirements were fully met.

BLM's Information Security Officer, Neil Brenner, has attended a number of accredited training courses delivered by URM. These have included the BCS 'Certificate in Information Security Management Principles' and the 'Practitioner Certificate in Information Risk Management'. Neil comments "Attending these courses and passing the associated exams has been beneficial, both in terms of better equipping me to coordinate the ongoing management of our ISMS and also from a personal development perspective. URM's training is delivered by experienced consultants. Their friendly, yet authoritative manner and extreme breadth of knowledge and experience in the subject matter makes them excellent trainers."

BLM has engaged URM to provide ongoing internal audit support to ensure this compliance with 'best practice' is maintained. BLM has been supported by a number of URM's consultants during the project, both in terms of providing consultancy and training support. "The strength and depth of the URM consultancy and account management team has been one of the key factors in ensuring the project's success" states Neil. "I have to say that the quality of the consultancy and training provided by URM has been exemplary."

> ***"The strength and depth of the URM consultancy and account management team has been one of the key factors in ensuring the project's success."***

Neil Brenner, Information Security Officer

BENEFITS DERIVED

Greater Client Assurance

Aligning to the 'best practice' guidance contained in ISO 27001 and ISO 27002 (Code of Practice) has simplified BLM's preparation for external security audits and reviews being conducted by key clients. Equally, the proactive and continuous improvement approach required by the Standard has resulted in a series of positive client comments.

Neil Brenner reports that "Whilst client reviews have always been positive, client reviews conducted since securing certification have elicited such comments as 'It was refreshing to see an organisation so in control of their operating environment' and 'BLM's information security management is head and shoulders above other organisations we have audited'. It is great to get such positive feedback and underpins the value of establishing the ISMS and targeting certification to the Standard."

Better Capture and Management of Information Security Incidents

Incident reporting is a good example of where improvements have been identified and where an improved structure has been created. For instance, BLM has established a portal where all incidents can be reported. The enhancements have led to an increase in incidents being reported, which in turn has given the Firm greater visibility of what is actually going on in the organisation. There is now a central view of potential vulnerabilities or threats that represent risks to BLM and its operational activity.

NEXT STEPS

Having successfully secured certification to ISO 27001 to its Birmingham, Bristol, Cardiff, Dublin, Leeds, Liverpool and Southampton offices. BLM is now emabrking on a programme of works which will see its ISMS scope extended to its newly acquired Edinburgh and Glasgow offices. The ISMS will continue to develop in response to any further expansion of the Firm, to support a programme of continuous improvement and in response to any changing requiremnts of the Standard.

> *"BLM's information security management is head and shoulders above other organisations we have audited."*
>
> BLM Client Review

BLM

T: 0161 838 6789
E: infosec@blm-law.com
W: www.blm-law.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