Not just your everyday accountant

brookson
Freedom to earn

BACKGROUND

Brookson, with its head office in Warrington Cheshire, is an innovative, market responsive provider of accountancy services to contractors, freelancers and self-employed professionals. Founded in 1995 by Rick and Carolyn Nevinson, Brookson currently provides a broad portfolio of financial services to 9,000 plus individual contractors, who work in a range of industry sectors including engineering, media, information security and healthcare.

The Brookson Team

Brookson was the first company of its type to offer daily and monthly account reconciliation and reporting. Accessibility is a key differentiator for Brookson. This relates both to its contact centre which is available 6 days per week and its market leading on-line services including real time accounting and tax updates. Brookson also prides itself on the employment law advice it is able to provide its clients. Through its team of 8 solicitors, Brookson is able to respond very quickly with tax advice to any changes in the legislative framework which will significantly impact its clients.

Underpinning Brookson's ability to maintain a reliable and legally compliant service delivery, as well as maintaining its very high levels of client satisfaction, is a significant reliance on IT systems. Brookson has invested heavily in systems which are used to collect, process and safeguard client information and deliver its market differentiating services. With this as a backdrop, Brookson identified securing certification to ISO 27001, the International Standard for Information Security Management as the ideal mechanism for demonstrating and maintaining a 'best practice' approach to safeguarding client data and the IT systems its services rely upon. This case study shares some of Brookson's experiences including business drivers, key implementation stages and benefits derived.

BUSINESS DRIVERS

The prime driver behind Brookson seeking ISO 27001 certification was an internal desire to adopt best practice in maintaining the confidentiality, integrity and availability of information and supporting information assets. Unlike many ISO 27001 certified organisations which are responding to pressure from one or a small number of key clients, Brookson has received no external pressure. It has proactively identified the importance of adopting a continuous improvement model in helping protect both its clients' data and company reputation. The ISO 27001 certification programme was initiated by Lee Kingshott, Information Systems Director at Brookson who submitted the business case to the Board. Despite some reservations based on the manpower requirements and time involved in maintaining a previous management system, the Brookson Board acknowledged the importance attached to and the benefits of developing a robust information security management system (ISMS). Achieving certification for the ISMS would be the most effective and tangible way of demonstrating both internally and externally how seriously Brookson takes information assurance. As Lee Kingshott explains "ISO 27001 is ideally matched to our business objectives and importantly it is not a prescriptive but a risk based Standard where the focus is on developing appropriate, pragmatic and proportional solutions."

KEY STAGES

Selection of Key Partners

Brookson was determined to own the development and delivery of its ISMS, but was keen to exploit the services of a consultancy and training organisation which was experienced in assisting organisations certify to ISO 27001. Lee Kingshott first encountered Ultima Risk Management (URM) when he attended one of the latter's ISO 27001 seminars and was impressed by the client centric and flexible approach of URM and the desire to make the Standard fit the organisation rather than the other way round. URM's certification experience and training skills were put to good use at the start of the certification programme with a high level presentation to the ISO 27001 project team, explaining concisely and effectively, the key stages and resource implications of certifying to ISO 27001. This was followed by a three day tailored training package extending the high level overview, introducing key information security management concepts and detailing key areas for a successful implementation.

As the project developed and moved into the latter phases, Brookson took greater ownership but always appreciated the fact that the consultant was available and accessible to provide advice and guidance. The consultant also played a useful role in attending the Stage 1 and 2 assessments and helping ensure the external assessor's requirements were fully met.

Brookson selected British Standard's Institution (BSI), partly because of previous trading relations but more importantly because having a BSI logo on the certificate would have greatest market recognition.

Scope of Certification

A great deal of discussion (facilitated by URM) and thought went into the process of deciding on the scope as Lee Kingshott explains "There was universal agreement amongst the Senior Management Team that the scope should be closely aligned to our business objectives and goals. There was also no dispute that ISO 27001 certification would be most appropriate for that part of our business focussed on delivering critical services to managed customers and protecting their data. With that in mind, Brookson determined the scope of certification to be IT Services. At the same time, we were set on ensuring that all staff would benefit and that there would be a consistent deployment of policies and processes and awareness training across all parts of the business."

Risk Assessment

Whilst Brookson, through its internal Prince Practitioners, had adopted risk based approaches across a variety of projects, no formal information security related risk assessments had been conducted. With the assistance of URM's consultant and risk assessment tool (Abriska), Brookson found the process valuable and beneficial. Brookson's risk focus up to that point had been mainly internal and the risk assessment provided a greater awareness of external factors such as environmental and legal. One lasting result of the risk assessment is an ongoing contact with the local meteorological office, local authorities, neighbouring organisations and local special interest groups.

A positive aspect of the risk assessment was the active involvement of the Senior Management Team, which as Lee Kingshott explains "ensured an iterative process was followed with considerable debate and discussion around risk appetite and what risk was acceptable. The final result was a risk treatment plan, signed off by the Managing Director, which helped in prioritising different treatment of risks. The adoption of Abriska was invaluable as a central repository and a generator of 'live' management information and ISO 27001 compliant reports "

Policy and Process Development

Whilst certification was limited to IT, Brookson was always determined to ensure all staff benefitted from the programme and that any policies and processes were implemented consistently and comprehensively across the organisation.

Lee Kingshott adds "It would be fair to say that Brookson had a comprehensive set of information security policies and processes prior to embarking on its ISO 27001 certification programme. However, following the risk assessment process, policies and processes were modified along with an updating of the staff manual, which is signed by all staff. What was interesting was that in some cases policies were relaxed. This enabled resource to be focussed elsewhere, in line with risk treatment priorities. One example of this was the Acceptable Use Policy, where the organisation adopted a more flexible and pragmatic policy surrounding the use of corporate PCs in lunch breaks for personal use."

ISO 27001 is ideally matched to our business objectives and importantly it is not a prescriptive but a risk based Standard where the focus is on developing appropriate, pragmatic and proportional solutions.

Lee Kingshott

Internal Communications and Staff Awareness

Even though it employs over 180 staff, Brookson still enjoys a close knit, family-oriented working environment. One of the Company's particular strengths is in its internal communications and delivering launch events/corporate messages. Thus, when Brookson was faced with launching the ISO 27001 Programme and presenting the importance of information security, it did so in its typically enthusiastic, fun and innovative way. Lee Kingshott explains "We used a variety of methods, including a Mastermind quiz where different departments competed against each other in terms of information security knowledge. We also created a cartoon character Larry, which appeared on 'Post-it' notes to reinforce good practice in areas such as clear desk and clear screen. Laminated mouse mats were also used to convey the incident reporting process. Presentations were also delivered by a member of staff who was able to communicate very effectively using non-management systems jargon and plain English, reflecting the existing culture of the Brookson organisation. Brookson also established an organisation wide Information Security Forum to assist in internal communications and staff awareness."

KEY SUCCESS CRITERIA

Senior Management Commitment

Lee Kingshott identifies the support and participation of the Board/ Senior Management as being key to the successful achievement of ISO 27001. Having determined that ISO 27001 is a risk based Standard with a focus on developing appropriate solutions that were totally compatible with Brookson's business objectives, there was total commitment from the Board. With the Managing Director Martin Heskerth and Lee Kingshott acting as sponsors, staff were in no doubt of the importance of the project to all staff.

Not Totally Top Down

Whilst having Senior Management support was critical, Lee Kingshott was keen to stress that staff at all levels embraced information security and the benefits it brought. Lee singles out the role played by the Service Development Leader at Brookson who acted as project champion and drove the communications programme. "Having worked in various departments across the organisation, she was able to tailor messages and deliver in a way that was totally accessible to the different audiences, as well as making the learning experience fun and enjoyable."

BENEFITS SEEN

Greater Awareness and Vigilance Across Staff

Whilst the certification scope was set as 'IT services', information security was always seen as having organisation wide importance which all staff would benefit from. Following the company launch event and a series of internal presentations, staff became far more aware of the importance of information security, as well as the potential impacts on Brookson and them as individuals if there was a breach of confidentiality, integrity or availability of information, particularly of client data.

Provided Validation and Consistency

Brookson had always treated information (and particularly client data) with considerable care and diligence. However, undertaking a formal information risk assessment with a third party risk specialist (URM) and the actual certification assessments, provided Brookson with validation that best practice was being adopted. The programme also ensured a greater consistency of policy implementation was achieved. The encryption of data was second nature to IT, but not necessarily for non-IT staff. Following internal training sessions, non-IT staff became aware of the risks and benefits attached.

Development of Improved Incident Reporting Process

One of the processes where there was real improvement was incident reporting. Prior to the programme, information security incidents had been reported along with other issues through the help desk system. However, in line with the continuous improvement 'Plan-Do-Check-Act' model advocated by ISO 27001, Brookson developed, in house, a new dedicated incident reporting process which was integrated into the corrective and preventive action process. Brookson has already seen the benefits of more incidents being reported, by all staff, leading to a range of improved information security controls including tightened physical access procedures for visitors.

Supplier Review

Brookson has also formalised its review process of suppliers and in particular its key suppliers. Whilst enjoying a close working relationship with its suppliers, Brookson has introduced a more structured review of their policies and processes, including tape back-up processes and the use of appropriate background checks on key supplier staff. Brookson has also encouraged those suppliers who are not certified to ISO 27001 to seek certification, or at least compliance, with the Standard.

brookson
Freedom to earn

T: 0845 058 1500
E: marketing@brookson.co.uk
W: www.brookson.co.uk

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