



ISO 27001 Case Study:



Kier Group plc

Background

Kier is one of the UK's leading and most respected building and civil engineering contractors. In addition to mainstream construction, the company offers specialist services around facilities management, private house building, commercial property development and project investment. The Group employs over 8,700 people worldwide and has an annual turnover in excess of £1.8bn. Kier Group was successfully floated on the London Stock Exchange in 1996 and since then has grown organically and by acquisition to become a leading force in the UK.

Kier takes its corporate management responsibilities very seriously and is committed to continuous improvement in all aspects of health, safety and environment. One of its stated core values is to 'be proactive, committed and safe'.

Business Challenge

In line with the Group's steady growth, its IT Function has expanded accordingly. Over thirty staff are employed at its Head Office with nearly fifty further staff working remotely with some responsibility in respect of the support of IT services. Heading IT is Terry Walker, Group IT Director, who has been with Kier for over six years. Terry has overseen significant changes in that time as the IT function has grown and matured. Arriving at Kier, he was aware that whilst the department was generally following good practice, there was a need for IT processes to be better structured and documented. As a result, various ITIL, Software Asset Management and help desk management initiatives were started. Internal audit reports, combined with a high level risk review, had also identified that the security environment could benefit from a more formalised and structured approach. Externally, Terry Walker was also conscious of the changing requirements and

demands, particularly of its Public Sector customers, where the Group was being increasingly asked about security, its approach and how it demonstrated best practice. Furthermore, in the cases of interoperability, *"information security was seen as paramount"*.

ISO 27001 Business Solution

In order to satisfy both internal audit recommendations regarding the security environment and to provide external partners with the necessary reassurances, Terry Walker identified certification to ISO 27001, the leading global standard for information security, as being the ideal solution. He believed that it satisfied Kier's information risk management and information governance requirements, but would not be overly onerous or administratively burdensome.

There was also no doubt in Terry Walker's mind about the benefits of certification over compliance. *"It was important to have an outcome at the end of the exercise, a recognised way of demonstrating best practice and this was an accredited registration certificate. The benefits and credibility that certification brings greatly outweigh the relatively small additional overhead involved."*

Furthermore, Terry Walker felt the ISO 27001 Standard realistically reflected the true scope of information security. *"Information security is a business not just an IT issue. Business is a lot more complex now. Internet connectivity has set expectations of information being accessible anywhere, anytime, and through any device. Security is not just about firewalls, it's just as much about people and process where awareness and training are key. It also needs to incorporate both internal as well as external threats to the business. All of this is reflected in the ISO 27001 Standard"*.

Certification Process

Having decided on the scope of the Information Security Management System (ISMS) Kier wished to certify, it enlisted the support of consultancy partner Ultima Risk Management (URM). An information risk assessment was carried out using URM's automated risk management tool. The risk assessment was reassuring in that no glaring security gaps were identified; no high risks were found which would have been a surprise, although a mixture of medium risks provided evidence that there was scope for improvements to be made to some of the existing controls. The risk assessment also confirmed that there was a need to introduce formal information security policies and processes that were better documented and structured, and more consistently implemented.

Reiterating Terry Walker's assessment that ISO 27001 is not just about IT, processes in human resources and physical security were identified as needing a more formal approach. The risk treatment stage naturally addressed these areas and following the creation and development of its ISMS, Kier Group was then assessed by BSI, the UK's leading assessment and certification body. In November 2006 Kier became the first major construction company in the UK to gain ISO 27001 certification.

Key Success Criteria

Terry Walker identified the following as being critical to the success of the project

- **Taking the business with you.** Whilst the ISO 27001 certification project was initiated by Terry Walker, he went out of his way to ensure the business (from the Board down) understood exactly what the Standard is about, as well as the benefits. Having representatives from all parts of the business on the Information Security Forum (the security coordination committee) also really helped to get buy-in and establish ownership
- **Internal champion.** Whilst Terry Walker was the project sponsor, it was essential there was an internal champion to act as an internal source of security advice and co-ordinator. The company did not create a new position but assigned the role to a newly appointed technical manager
- **Experienced and approachable partners.** A vital ingredient in achieving certification was the selection of the right consultancy partner and certification body
- **For the former, Terry Walker chose Ultima Risk Management.** The company was already known to him and he felt was of the right size, "big enough

to offer resilience and specialism but small enough to be personable and approachable". The track record of both the company and the designated consultant were also of paramount importance in order to avoid common pitfalls and make sure timely progress was being made. Terry Walker was also keen to work with a company which is committed to knowledge transfer and "training our team to develop their security skills and enable Kier to become as self sufficient as possible."

- **Kier chose British Standards Institution (BSI)** as the certification body on the grounds that a strong relationship already existed between the two organisations and that "*they really understood us*". Terry Walker was impressed by the realistic and pragmatic approach of the assessor. He also strongly recommends early engagement with the assessor (possibly through a pre assessment day) "to help build a common understanding, ensure the project is on the right track and to ensure there are no surprises at the certification stages!"

Benefits seen to date

Since certification, Terry Walker can point to a number of tangible benefits that have emerged.

- "*There has been a significant change in attitude and heightened security awareness within all staff in Group IT (e.g. PCs being locked when the user is moving away from his or her desk as a matter of course). The Group IT Steering Committee has also embraced information security wholeheartedly and security is now a regular feature at meetings*"
- "The need for documentation provides a very real and physical proof that something has been done (e.g. a test recovery has been completed)"
- "*The fact that an external assessor conducts regular assessments keeps everyone focussed and on their toes. A definite advantage over compliance!*"
- "Being the first major construction company to achieve ISO 27001 not only provided Kier with a competitive advantage in the market but was a real fillip and morale builder for the Group and the IT department in particular. To commemorate the achievement all the team members were given Kier umbrellas with the ISO 27001 logo on!"
- Overriding everything, Kier can clearly demonstrate to all key stakeholders that as far as information security is concerned it is doing everything it can to uphold its core values of being 'proactive, committed and safe.'

GETTING THE BALANCE RIGHT.

URM

ULTIMA RISK
MANAGEMENT

Ultima Place, 448a Basingstoke Road
Reading, Berkshire, RG2 0RX

Phone: 0845 838 2084

Fax: 0118 902 7451

www.ultimariskmanagement.com