



Specialist services and solutions for IT governance,
risk management, compliance and information security.

Case Study



IT Governance smoothes the way to ISO27001 certification for IMS Hospital Group

Pharmaceutical data provider, IMS Hospital Group, needed to achieve ISO27001 certification in short order to meet the requirements of a potential provider of valuable market information. With the support of IT Governance's consultancy, training and specialist compliance products, IMS was able comfortably to meet the requirements of its two-stage audit, despite a demanding time scale.

BACKGROUND

The success of a pharmaceutical company depends on long-term, complex drug development, patent protection and good patient safety records. Inevitably, the risk of litigation in all these areas is a real business issue. Data security is therefore a significant concern, and robust, effective measures are required to keep an organisation's information watertight and to limit its exposure to legal action.

As a significant source of sensitive industry data, IMS Hospital Group ('IMS') is subject to the same stringent demands as its pharmaceutical clients and, in common with other organisations, is experiencing growing pressure to demonstrate good practice in information security.

IMS was already subject to its parent company's strict privacy and data protection policies. However, a potential new source of data, a government health organisation, stipulated that IMS should also be certificated to ISO27001, the global best practice standard for information security management.

IMS recognised that, as well as satisfying the immediate demands of this particular organisation, ISO27001 certification would be a source of reassurance to others. While its parent company already had externally audited policies, independent confirmation that IMS maintained best practice information security could only add to its own reputation, helping to attract future contracts and information sources.

REQUIREMENTS

As IMS had no existing internal knowledge of ISO27001 certification, in early 2007 it appointed IT Governance to undertake an initial appraisal of its needs and advise on a course

of action. As IMS's ISO27001 compliance project manager Chris Lofts confirms, the company was quickly convinced of IT Governance's expertise in the area,

'Through our phone calls and subsequent meeting, it became apparent that IT Governance had a real depth of expertise in ISO27001 and practical experience that was very relevant to our situation.'

PROCESS

Guided by IT Governance's outline recommendations, IMS initially set about pursuing ISO27001 compliance as an in-house project.

The work of the IMS team was aided by two products from IT Governance's range of specialist compliance tools: risk assessment software tool, RA2, the Art of Risk, which is designed to enable businesses to undertake an information security risk assessment that is compliant with the Standard; and the ISO27001 ISMS Documentation Template Toolkit, which supplies prewritten policies and procedures designed to fast-track any ISMS project. The company also called in a consultant from IT Governance on an occasional basis, to discuss and advise on particular aspects of their programme. The consultant also advised IMS on how to make best use of its RA2 software and ISMS Toolkit, helping to tailor these to the specific needs of the organisation to speed the compliance process.

However, a change in priorities within the business meant that IMS was suddenly placed under even greater pressure to achieve its ISO27001 certification, with the deadline brought forward by almost three months. At this stage, it was decided to engage IT Governance on a more intensive basis, so as to accelerate IMS's preparation.

The new engagement began with a strategy and planning session, at which both companies worked together to agree the roadmap for the project and milestones at various critical stages. As part of this process, it was also necessary to assess the current skills and knowledge of the IMS in-house project team.

As project manager, Chris Lofts had recently attended two of IT Governance's expert training courses: a three-day ISO27001 Implementation Masterclass and an ISO27001 Internal Auditor Course. The Masterclass included a very relevant study of accelerated certification projects, which enabled Chris to appreciate some of the pressure points and issues that were likely to occur. However, to extend relevant skills to other members of the team, it was decided that IT Governance should also put IMS's internal quality management system auditors through an ISO27001 Internal Auditor Transition Training Course.

IT Governance's experience of guiding many other businesses through information security certification proved very helpful, as Chris Lofts explains, 'The correct approaches for ISO27001 compliance are not immediately obvious from reading the Standard alone. It was immensely useful that IT Governance could talk about its experiences across various industries and advise on practical approaches that would offer the most efficient route.'

At this stage, the IMS team was ready to tackle its tasks in a concerted fashion. However, the IT Governance consultant maintained contact with Chris Lofts throughout and visited the company again at each of the project milestones, so as to sample and review the team's work and provide guidance on various aspects of the implementation. The consultant also helped IMS undertake a dress rehearsal prior to its Stage 2 audit, which ensured that the company was as ready as possible for external scrutiny.

OUTCOME

IMS's Stage 1 audit took place in February 2008, when auditors from BSI visited to inspect the company's ISO27001 documentation. The visit passed off entirely successfully, and IMS was advised that it should proceed to a Stage 2 audit in April, when BSi would subject the company to far greater scrutiny on how its policies and procedures were applied within the business.

This second audit proved similarly successful, with only one minor non-conformance identified that was swiftly corrected by the IMS team. The company went on to receive its ISO27001 certification that same month, fully achieving the demanding challenge it had set itself within the revised, tighter timescale.

Looking back at the project, Chris Lofts says that IT Governance provided invaluable support to his team, 'They understand the subject matter both at a theoretical and practical level, which helped guide us to the approach that would get us there fastest. We might otherwise have gone about things in other ways, which would have made the deadline impossible to achieve. The other important point was that IT Governance gave us everything we needed, from advice, to training, to purpose-built tools – that covered off all our needs very quickly and meant we had more time to spend on achieving our goal.'

He also emphasises that IT Governance's support goes further than just enabling a successful certification, 'Rather than saying "Let's just get through the audit", IT Governance approaches the certification process from a standpoint of real-world business benefits, and has helped us make it a part of how we approach our work."

Being ISO27001 certificated has added significant value to IMS's business. Not only has it gained an important data supplier, but, as Chis Lofts says, 'It demonstrates to all our suppliers and clients that we uphold best practice, and underwrites the quality and integrity of our finished product.'

Just as we have helped IMS Hospital group achieve ISO27001 compliance on time and within budget so we can help you. **Call us now on 0845 070 1750.**

About the IMS

IMS Hospital Group is a specialist market research company that provides data and consulting services to the pharmaceutical industry. Its databases provide insight into key therapeutic areas, such as oncology, thrombosis and stroke, as well as into hospital pharmacy prescribing activity. It is part of the global group, IMS Health, which prides itself on being the world's single source for pharmaceutical intelligence, with almost every major pharmaceutical and biotech company a customer.



™ About IT Governance

IT Governance has substantial real-world experience in designing and implementing IT GRC-related management systems. Founded in 2002, we are a professional services company with a wealth of consultancy skills that originally focused on information security/cybersecurity standards, notably ISO27001. We have an impressive track record of more than 100 consultancy clients successfully certificated to ISO27001 alone.

We have since developed our offerings into various other management disciplines and now provide a comprehensive single source of information, advice, books, tools, consultancy and training for IT governance, risk management, compliance and IT security.

Flexible service package

The IT Governance professional services provide you with the chosen level of support you require. This is true whether you seek a certification to international standards, based on the findings of the initial scoping phase and compliance with the agreed resource and project plan, or whether your aim is to follow best practice and 'compliance'. We recognise that no two situations are identical. Therefore, we tailor our services and solutions to meet your needs.

Risk management

Risk assessment is the core competence of modern business. In line with the Sarbanes-Oxley Act, Basel II and III, ISO31000, ISO27001, and OCTAVE requirements, we help you to formalise and structure your approach to strategic and operational risk, fully-incorporating cybersecurity into the picture. Our unique approach takes into account the complex competitive, regulatory and environmental factors that affect achievement of strategic goals. Our services can include the development of a corporate risk log, and risk assessment through to the production of formal risk treatment plans and review processes.

Ongoing support

IT Governance believes that serving you well means helping you to develop the skills and knowledge necessary to run your own management systems and compliance programmes.

Our clear focus is therefore on developing your skills and confidence. Through our empowering value-for-money approach, you can encourage and enable your people to take ownership of the resulting arrangements and improve performance across the organisation.

Single source

You and your lead IT Governance consultant will have access to the comprehensive and integrated resources, available from IT Governance, to ensure a successful project. These include:

- Risk management expertise
- Technical information security expertise
- Trainers (practitioners) and training courses (see the training pages on our website)
- Books and tools available through our on-line shop
- Recruitment support for IT governance related posts

Phone: +44 (0) 845 070 1750

E-mail: servicecentre@itgovernance.co.uk

Web: www.itgovernance.co.uk

