Case Study

Healthcode passes its infosecurity medical with the help of IT Governance

Information security is not only headline news these days; behind the scenes it is becoming an essential requirement for an increasing number of organisations seeking new business. One SME in the health sector decided it had to be prepared, and turned to IT Governance for help.

BACKGROUND

You can hardly open a newspaper these days without coming across another tale of lax information security. Lost laptops containing sensitive data, disks going adrift in the post, customer databases being hacked – it all adds to the pressure on companies which have to handle personal data on a daily basis.

Against this backdrop, organisations are increasingly seeking guarantees from their suppliers that the information they handle is secure. Being able to demonstrate this is a hurdle suppliers need to tackle to ensure they continue to win new business.

Healthcode, the UK's largest electronic health billing specialists in private medical insurance, have always been aware of this. Recently, however, they decided they needed to improve further their already high standards by applying for accredited certification to ISO27001, the global standard for information security management.

"Security is at the heart of what we do," said Steve Carroll, Healthcode's Managing Director. "We're processing highly-sensitive personal information, whether in the transfer of an electronic bill from a provider to an insurer, or through other services, such as secure e-mail or practice software for specialist.

"We've always taken security seriously, and even before we went for the formal ISO27001 audit, we always operated pretty closely to the earlier version of BS7799 standard on this."

REQUIREMENTS

"We had always stopped short of being audited because of the overhead involved. However, as we've grown and wanted to demonstrate that we deliver world class security, the best way to do that was to 'get the badge' and let the world see we've got it. For our core billing business, this is a way to underline our seriousness about customer care; for the new services we want to introduce in future, it is more about giving Healthcode a competitive advantage to win new business."

"Information security has raised its profile over the years; in particular, if we want to do anything in the public sector that would be the first thing they would look at," said Steve. "If we ever do work with the NHS, it's a signal that a small private company like ours competes on equal terms with larger operators."

PROCESS

To get the process of building an ISO27001-compliant Information Security Management System (ISMS) underway, Healthcode turned to risk management and compliance specialists IT Governance.

From the outset, Healthcode showed it was serious by giving the project backing from senior management and appointing a dedicated project manager, Raj Patel, to oversee the process.

Raj, who had only recently joined the company and had no previous experience of information security, promptly booked himself onto a ISO27001 foundation course run by IT Governance. This gave Raj a bedrock of knowledge on which to build Healthcode's compliance project, and to assist him over the following months, the company also purchased 10 days of IT Governance's consultancy time.

The IT Governance consultant guided Raj to formulate the policies and procedures appropriate to Healthcode's size and business, and also guided him in the use of vsRisk, IT Governance's specifically designed ISO27001 risk assessment tool. vsRisk radically simplifies the process by which risks and appropriate control measures are identified, and Healthcode's resulting risk assessment was singled out as "noteworthy" by the independent assessors – high praise indeed in such a situation.

In the risk assessment phase, Raj was supported by five colleagues drawn from across the business. To ensure that they had the necessary knowledge and skills, IT Governance ran an accelerated ISMS internal auditor course for them, compressing into a single day all they needed to know.

However, when an ISO auditor arrived in January 2009, Raj got a shock: "I thought it was just going to be a gap assessment. It turned out to be Part 1 of the actual audit process, the document review. He sat down with me for the whole day. But it went pretty well because I was well organised, with all the documentation and records prepared."

IT Governance then conducted a pre-certification audit – essentially a dress rehearsal – in March 2009 that gave the Healthcode team an idea of what to expect on the 'real thing'.

"It is a question of knowing what to expect," said Steve Carroll. "I've been through ISO9001, but this was much more thorough. The rehearsal basically put you on notice that you were going to be asked some fairly searching questions."

OUTCOME

All the preparation paid off: the two-day second stage of the audit in April passed off remarkably smoothly, without any non-conformance being uncovered by the external auditors.

NEXT STEPS

Now that accreditation has been achieved, how does Steve plan to bring it to the attention of current and prospective customers? "We'll probably make as much noise as we can, to be honest," he chuckled. "We will incorporate the badge on the bottom of e-mails, we'll print it on our letterheads and compliment slips, and all the proposals we offer to the industry will include the badge."

He sees ISO27001 not so much as a competitive advantage as an increasing necessity. "It's something that allows us to toe the line in order to compete. I think there will be selection procedures in future where it will be a filter – the client won't talk to anyone who doesn't have the appropriate certification.

"IT Governance helped us create an information security management system that's compliant with ISO27001 and yet proportionate for a smaller business. In terms of value for money, expertise and a non-bureaucratic approach, IT Governance came up trumps. We have been very happy indeed with the outcome and have recommended the company to others."

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