

– 3net

CASE STUDY: ISO/IEC 27001

3net is a UK based IT consulting company established in 1999 and one of the UK's fastest growing providers of infrastructure management services. With a portfolio encompassing IT security and application acceleration, 3net consultants are involved in all aspects of their clients' business from network design, customer network support, improving web based performance through to providing IT security solutions such as intrusion detection and firewalls.

With security an inherent part of its service solution and particularly in today's security-conscious climate, it was recognised that for the company to continue to grow, it really needed to demonstrate its commitment to the safe and secure management of assets belonging to both clients and company.

While the company had suffered nothing worse than an attempted break-in at its Chertsey headquarters, it made sound business sense to have a robust and well rehearsed plan for managing all aspects of its security. With this in mind, the company's security officer, Stuart Brown began putting together a business case in December 2005 for implementing an information security management system (ISMS) with certification to ISO/IEC 27001.



Benefits

Commercial impact

Protecting existing revenue while attracting new business was the starting point of the whole project. And while still early days, 3net is using its successful certification as a market differentiator to strengthen its reputation, particularly when targeting the governmental and corporate sectors.

"We can now talk from a position of strength having gone through system implementation ourselves. It has impacted on the way we specify our technical solutions and helps when designing systems."

Asset management

The company now fully understands what assets – people, software, information and data – it owns and controls and the importance of each of these to the company. Drawing up a full list of assets is an important part of risk management, but brings additional benefits in terms of sharper business focus.

Raising awareness

The nature of its business means there's already a high level of security awareness. However, having implemented ISO 27001, this has increased further, particularly amongst office based staff. Publicity in the early stages



of the project, meant that all employees have been kept informed throughout the project. However, as Stuart Brown, the company's security officer is only too aware, the real challenge will lie in sustaining this level of awareness.

"We attend team meetings, use newsletters and emails to keep awareness high and it is working. We are all more security conscious which can be seen even in the simple, mundane things. If I forget to lock my PC when I leave my desk, someone will notice and remind me. We've bought a high capacity shredder which people will use when they need to, rather than leaving paperwork in a pile for shredding later."

Continual improvement

The project team really began to use internal audits as a diagnostic tool to look at aspects of its business and compare with best practice. "Placing a spotlight on internal processes and procedures will inevitably identify areas for improvement, and so it did with us. We put in stronger encryption to protect the wireless set-up within the office as a direct result of an internal audit; as well as improved back-up processes."

Lloyd's Register Quality Assurance is a member of the Lloyd's Register Group



LRQA
Measure the Difference

“Using bespoke software, I was able to quantify the benefits and show that undertaking the project would pay for itself within two years – senior management agreed.”

Stuart Brown, Security Officer, 3net

Getting the Board on-board

Responsible for developing security solutions for 3net, it quickly became apparent to Stuart there were significant business gains to be made from certification to ISO/IEC 27001.

There has been a growing expectation from both government and corporate sectors – particularly those who were already operating an ISO 27001-certified ISMS – that their business critical supply chains would at least be compliant with the standard, and better still, able to show external verification from a third party.

To gain top management support, Stuart wrote a business case clearly outlining

quantifiable benefits of seeking certification. He looked at the revenue streams from those clients most at risk if 3net were not to take the certification route and using even a conservative percentage swing found that the cost of implementation and certification was clearly outweighed by the potential loss to business.

The Board agreed and set the goal of gaining certification within 6 months. Why such a tight timescale on the project? “We’re a small company employing less than 40 people and simply couldn’t afford for a project to drag on for months,” explains Stuart.

“LRQA was recommended to us. However, we needed to be sure that it was the best fit for us. Having looked independently, we knew LRQA had a strong reputation in this area. We then met with an LRQA account manager who took us through the certification process which gave us the confidence to go forward.”

Strategy: first steps

Stuart had been involved in security most of his working career however had little or no experience of implementing an ISMS therefore bringing in an external consultant seemed a logical decision, particularly given the tight timeframe.

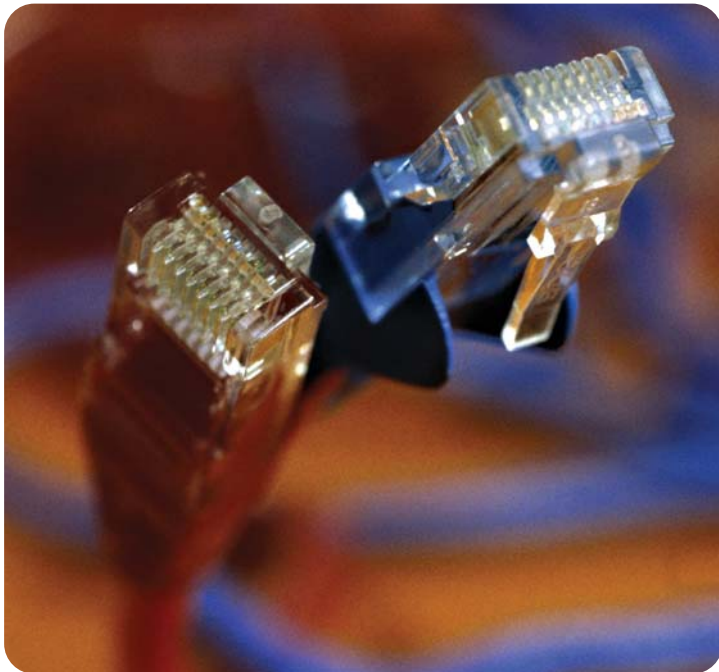
3net settled on using Red Island Consulting. Their first task was to carry out a gap analysis to establish the processes and procedures already existing within the business. This would give an early indication of any business issues needing to be addressed and also the potential scope of activities needing to be covered by any certification.

The results weren’t quite as expected. “We assumed we would have a lot of ground to cover. However, it turned out we were already doing a lot of what

was needed but couldn’t demonstrate this through our documentation,” Stuart explained.

“Importantly however, the gap analysis proved to us that certification was an achievable and very realistic aim. We had established where we were and what needed to be done which meant we were comfortable in taking the decision to include all our business processes within the scope of certification.”

A project team was formed to include Stuart as project manager; the Office Manager who had access to the accounts system, company records and personal data, much of which was sensitive; and a Director and founding member of 3net with overall responsibility for IT operations and security.



LRQA
Measure the Difference

Assessing and treating the risk

In April 2006, 3net undertook a full risk assessment using the Red Island methodology. The structure of this approach enabled the company to very simply categorise its risks with a value of 1 to 5 allocated to each of the identified actions. Those marked '5' – which were the highest priority – were dealt with first.

The output from the risk assessment translated easily into the risk treatment plan, which gave a clear picture of the organisation's business risks and how well they were dealing with them.

Reflecting the results from the initial gap analysis, lack of documentation proved the most significant finding although other areas included security protocols surrounding encryption of sensitive information on consultant laptops and further development and testing of 3net's business continuity planning.

However, the results gave 3net confidence they were along the right track. Despite this, there were still over 100 actions to be dealt with and the project team had agreement from the directors to allocate whatever resource was needed. This enabled them to spend the necessary time working through the priority actions in readiness for the Stage 1 assessment from LRQA in July.

Certification: Working with LRQA

The previous few months had seen a number of audits carried out on company activities. Two of 3net's major customers had carried out second party audits and Red Island had undertaken a few 'dummy runs.' This had given the project team a better knowledge of the auditing process and an expectation of what the external audit might be like.

"Our consultants had advised us that LRQA assessors were trained to give practical advice and that we would actually find the assessment a useful learning experience. However, despite this we were still expecting something of a dry, factual audit."

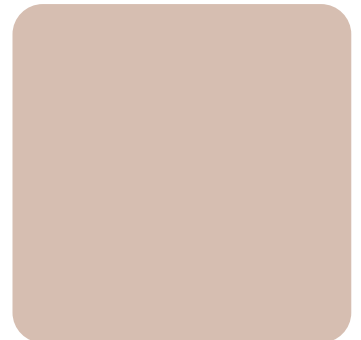
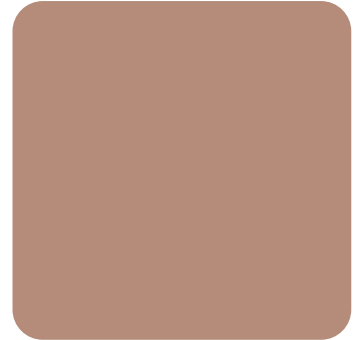
The reality was a little different however as Stuart explains. "Our assessor had a good, very open interviewing style which helped put our people at ease. We didn't at any time feel we were being grilled."

However, one of the most useful elements of the assessment was the pragmatic advice that their assessor brought with the ability to illustrate with anecdotes and examples from many years experience of working with all types of organisation.

An example of this was in the opening meeting of the first visit, where Stuart advised their assessor they were thinking of adopting ISO 9001.

"He drew up the two standards on a board, showing the common elements of the two standards, giving some advice on how we could organise a system to cope with quality in addition to security.

"This was something that really stuck in our memory. This has allowed us to develop a template to audit both security and quality elements on supplier sites should we want to."



"We found the 'mentoring' support from both our consultant and our LRQA assessor invaluable. Knowing why you're doing something is so important and knowing that you're managing it in an appropriate way is a confidence booster."

3net

CASE STUDY: ISO/IEC 27001

www.lrqa.co.uk



Learning points

3net went through an intense implementation period throughout which time they were on a steep learning curve.

Whether it was revisiting their business continuity planning, learning to write effective policies or using internal audits as effective business tools, the project team succeeded in achieving ISO 27001 in 6 months.

But would they have done anything differently? The project team offer an insight into their experiences with their key learning points.

- We undertook the majority of work ourselves although took guidance from a consultant and our assessor.

From the outset, we had booked our consultant for around a day a fortnight at 'critical' points along the way. The initial stages – risk assessment and business impact reviews – were relatively straightforward.

It was during the later stages when we were managing the system, carrying out audits and conducting awareness sessions that we really needed more support.

It was the combination of using unfamiliar skills and maintaining the system that caused pressure. In hindsight, we could have made it easier on ourselves.

- The tight 6-month timeframe didn't allow for us to consult

widely with our staff. We are a small company and our people understood why we were taking this route. However, more time may well have allowed us to build greater consensus and a greater feeling of ownership.

- A project team of three people was ideal for our size project and company. Additionally, having a Director on board speeded up decision making.
- We used LRQA assessments to help us further improve. We were able to tap into our assessor's practical experience from visiting many different types of organisation and use his knowledge to start thinking about how we could integrate quality requirements.
- Internal audits became a good business tool to help us identify those areas we could bring about real change and improvement – such as backup

processes, encryption, stricter control over third party processes, etc.

- We chose this time to automate certain tasks such as password management, and enforcement of virus updates, etc. The standard requires these are done on a regular basis but they can be labour intensive. Automating as much as possible enabled us to work more efficiently.
- Auditing has proved a useful skill to learn. We now regularly audit our sub-contractors and we've highlighted areas of concern – such as the need for a business recovery plan - which have now been addressed.

This has actually led to our contractors having a keener understanding of our business, and the environment in which we work which in turn has led to a stronger working relationship.

LRQA

LRQA is one of the world's foremost certification, training and verification organisations, having provided independent assurance of management systems for many years.

Service options include a range of business assurance activities, from third party certification of complex integrated management systems through to auditing of simple, standalone systems.

More on: www.lrqa.co.uk

Articles, case studies and information on LRQA assessment and training services can be found on our website in addition to links to other useful Internet-based data.

More on: www.redisland.co.uk www.3net-uk.com

Contact Us

Sales

T 0800 783 2179
F +44 (0)24 7630 2662
E enquiries@lrqa.co.uk

LRQA Training

T 0800 328 6543
F +44 (0)24 7651 1116
E lrqatraining@lrqa.com

Technical Helpdesk

T 0800 9000 12
F +44 (0)24 7630 5533
E technical-helpdesk@lrqa.co.uk