Blackmores

ISO 27001 Case Study

Anton Group ISO 27001 Implementation

There is rising awareness of information security issues within the print sector and no where is this more apparent than with those printers who offer a design to despatch service. Organisations like The Anton Group who have the in-house capability to manage large scale mailing projects and can enclose and mail over one million packs per day and handle a large amount of personal and sensitive data.

Having worked for some years with a number of well known High Street brands and financial organisations, The Anton Group had well established security protocols in place with audits from clients a regular fixture in the working calendar. However, it also recognised that it could improve and the long term aim was to formalise the security processes it had by implementing an information security management system.

Recognising that a limited number of print companies had taken this step, they spotted an opportunity to differentiate Anton in the marketplace and gain an important edge over its competition. It wanted to improve internal processes and in doing so reduce the risk of security breaches and raise confidence in its ability to manage operational risk. By implementing a strong ISMS and adding ISO 27001 to its roll call of certifications, they felt able to better protect its position as a one-stop print and mailing solution provider.

The organisation already operated an integrated quality and environmental management system certified to ISO 9001 and ISO 14001. Well aware of the value of a management system based structure, the IT Manager and Facilities Director were thinking long term about the value of introducing an ISO 27001 approved information security management system. However, with the beginning of the recession, the project had been put on the back burner. That is, until a security audit from a major financial auditing organisation on behalf of a leading High Street bank brought it back on the agenda.

Security audit prompts rethink...

In 2008, a major financial auditor visited Anton to carry out a security audit which was broadly based on the key requirements of the international ISO 27001 standard. However, as Kim Scott, Facilities Director explained, they weren't fully prepared for the audit.

"While we were performing reasonably well having already carried out a lot of work in tightening up our processes and putting procedures in place, we were falling down in documenting what we were doing. We really needed to formalise our processes. While we were covering the key requirements of the standard, we were doing it on an informal basis. So, following this initial client audit, we set about improving our security standards and more importantly keeping a clear audit trail."

Once the necessary changes had been put in place to satisfy their client's security requirements, it seemed a natural progression to look again at the feasibility of becoming certified to ISO 27001.

While Kim Scott and IT Manager, Paul Dickerson had gone a long way towards putting the necessary processes in place, they also recognised they needed a management system to pull their processes together and to plug any gaps. The Board agreed and set the objective of gaining certification as quickly as possible. This meant the team needed to bring in expert help to guide them through the project to completion. They began to look for a suitable consultancy which had experience of implementing an ISMS within the print sector.

It was at this point that the project began to stumble as Kim explains. “We interviewed a number of consultancies to help us but they seemed more interested in selling us their formula than fitting in with our needs. They were giving us timescales of between 12-24 months to completion but were not taking into account the work that we had already completed. We had already satisfied our client audit so knew we were a good way towards meeting the requirements of ISO 27001. However, we didn’t understand what was needed on the documentation side of things and it was here that we needed guidance and coaching. There were some grey areas for us,” explained Kim.

It was at this point that they contacted their LRQA Account Manager, Mark Dougan. “We spoke with Mark on a couple of occasions about the areas we were most concerned about. Shortly after, he visited site and was able to have an informal look over the system. The advice he was able to give gave us the confidence that while we were on the right track and the main controls that we had in place were fine in principle, there were gaps needing to be plugged.

“Policies and procedures needed to be written. We needed to devise a sensible approach to managing our risks which meant a formal risk methodology was needed. While we could have worked through these elements in-house, it was felt that with the timescales involved, we really needed expert help,” said Kim.

Following the visit, Anton employed a consultant to produce the documentation and provide guidance on managing risk.

A minor glitch...

Senior management commitment had been a key driver behind Kim and Paul’s goal in getting early certification. This commitment from the top was used to the implementation team’s advantage by driving through the necessary changes. This included initiatives such as blocking all USB ports on every PC in the building. This meant that staff had to gain senior management approval for any use of a memory stick which would only be granted if there was a legitimate business reason. Access to personal emails and social networking sites were also stopped completely with restricted access to other websites.

The need for these new restrictions was understood and accepted by the employees. Previous client audits which had taken all aspects of Anton’s operation into account had already instilled the need for tighter security into the minds of each member of staff. This meant that Anton employees not only understood the need for the constant revision in security policies and were happy to make the changes but also to become more involved by suggesting ways to further improve security.

The tight timescale that Kim and Paul were working to had also created pressure on assessment dates. Again, the team contacted their LRQA account manager and were fortunate enough to get a cancellation which meant they were able to book the first part of their external assessment at short notice. With the Stage One visit in the diary, they had just a couple of months to put in place the final procedures and appropriate documentation for their information security management system. At this point, they had been able to source a consultant who was working with them in putting a system in place.

However, not everything was to go quite as smoothly as Paul Dickerson, IT Manager explains. “We were confident that we had everything in place for our first assessment visit and that the documentation was robust and thorough. However, our LRQA assessor didn’t agree. He felt that the initial approach we had taken just wasn’t up to scratch. We weren’t expecting this. It meant we had to rethink our approach.”

Far from placing the project on the backburner however, this setback refocused the team’s thinking. A new consultant, Mrs Melanie Blackmore from specialist security consultancy, Blackmores was appointed and work began almost immediately on making the changes necessary, and importantly in time, for the next visit just three months down the line.

Spreading the word...

The LRQA Stage One assessment visit had shown weaknesses within the approach that had been taken but it was also recognised that the system was actually fundamentally sound as Paul Dickerson, IT Manager explains.

“While we were disappointed with the outcome of the visit, we knew that the issues could be resolved and that we were simply at a different stage in the process. We had taken the decision to appoint Melanie Blackmore to give us the guidance needed to fill in the gaps and from this point we didn’t look back.”

The change in consultants gave the team a new impetus. Melanie started off by giving a high-level briefing on information security to all Board members. “I find that typically it is very difficult to gain access to senior management and so having a two hour briefing session with the Anton Board was testament to the importance they place on this project,” explains Melanie. “It was clear they were fully supportive. I was able to get valuable feedback from them on what they believed the greatest risks were to the business in terms of reputational damage and how these could be mitigated.”

“One of the key challenges for Anton was to simply get the message across in a relevant and appropriate way to make sure of understanding and buy-in from all employees. The message and method changed depending on the teams involved. For example, the message to the finance team was that getting this certification would have benefits in reduced insurance costs. To the sales and marketing team, it was the potential of winning new business and also increased assurance of keeping existing clients.

“Implementing a management system within a manufacturing environment brings its challenges. With the shift system in operation, we had to find different ways of getting the message across as it just wasn’t possible to get everybody into a classroom,” Melanie explained.

This included initiatives such as ‘toolbox talks’ which were debrief sessions to keep all machine operators up to speed with the changes. These also gave a valuable opportunity for any ideas to be fed back to the implementation team with ideas on how to further enhance security brought into working processes. Likewise, throughout the organisation, departmental heads were fully briefed to cascade information to their teams.

Documents such as non-disclosure agreements were placed in payslips together with an explanation of the need for new procedures. Posters explaining the reasons for the changes in processes were printed and placed together with copies of the security manual in common areas. Critical suppliers, such as agencies supplying contract staff, were also audited with all suppliers contacted to ensure they were aware of their responsibilities under the revised security requirements.

A security culture...

The change brought about by the implementation of the information security management system has been one of evolution rather than revolution. The client audits had already seen Anton introduce tougher security processes throughout its operations particularly in the area of data management. However, all aspects of internal security have been revisited and tightened where needed. All tasks are now documented and careful records kept on site. There are increased vehicle registration checks at the security gate, passes for vehicles on site, it is mandatory to sign the visitor's book and all visitors are escorted while on site.

The changes have been extended to include new employees as well as existing staff. Security now forms a part of the revised New Starters Induction which sees all new employees learning about the company's security policies, about the use of security cameras and restricted access to areas containing sensitive material.

Paul Dickerson explains further. "All staff are now more aware of the need for security and importantly why we are bringing about these changes. The journey towards certification has made everyone aware of the role they have to play.

"The impact of the recession has only helped to reinforce the message. It's brought an awareness of the need to differentiate our business from the competition and the impact this could have for the future growth of the business. We believe it will also encourage companies to give us a larger share of their business while also attracting new clients wanting to use one of the handful of commercial printing companies in the country with an ISO 27001 certification."

Certification and beyond...

Anton already had ISO 9001 and ISO 14001 systems certified by LRQA and it therefore seemed a natural choice to use the same assessment body when it came to ISO 27001.

Kim Scott takes up the story. "LRQA are recognised as one of the country's leading certification bodies and are respected throughout industry. It made sense when choosing an assessment body to work with to opt for one we knew and trusted.

"Our LRQA assessor, Malcolm Newman led us through our first visit with a helpful but strong commitment to the certification. His comments and guidance made us look again at our approach and improve on what we had - particularly with the review of risk assessments and records.

"In the final assessment, he was practical in his ability to see the way we operated as a manufacturing plant and how that related to security. The comments that he made enabled us to make improvements in a number of areas, for example in the calculations that we used to work out residual risk and in how we handle the retention of customer data.

"Malcolm was extremely experienced and thorough. It meant that when certification was recommended following our second stage visit, we could be confident we had a strong system. And on our most recent surveillance visit, Malcolm was able to see the improvements that we had made, while pointing out where we needed to improve further," concluded Kim.

Certification to ISO 27001 had always been the goal that the Anton team had in mind from the outset. It is an assurance to clients – and importantly potential clients – that the company has a security programme that has been externally recognised as meeting the requirements of an internationally recognised and trusted standard.

Learning tips...

Are you considering implementing a certified information security management system? In this section, Paul Dickerson and Kim Scott of Anton offer their 'tips' for other organisations considering an ISO 27001 approved system. We also offer the consultant's viewpoint with Melanie Blackmore of Blackmores offering some pointers.

Paul Dickerson, Kim Scott...

- Ask yourselves some basic questions: why do you want certification? Will it be driven from top management? Research everything and always ask advice.
- Don't be afraid to speak to your assessment body from the start. We spoke to our Account Manager before starting on certification and found him full of good advice and encouragement.
- Search for a good consultant. Your certification body will give you a list of people they deal with. Interview them and decide who you can work with. Are they just interested in the money or a long term partnership?
- Set up an enthusiastic ISMS Project team and involve your employees from the start. Get them on your side and once you start, keep them involved all the way.
- Your assessor is on your side. Don't be afraid to ask questions if you don't understand. They want you to succeed in the certification.

Melanie Blackmore, Blackmores...

- Communication is vital when implementing any management system. All those involved in the process need to understand the benefits because if they don't, they will fail to buy-in.
- The process owners are key. They know the risks better than anyone else as they deal with them on a day-to-day basis. They can identify opportunities to bridge gaps and so reduce risks.
- Make sure you have effective communications channels once the system has been embedded to ensure a high level of compliance and improved controls.
- Certify your system. There are lots of organisations who claim compliance and have an Information Security policy but play lip service in order to respond to tenders. Achieving certification demonstrates confidence to stakeholders and is something that you can be proud of and promote to existing and potential clients.
- Train your employees. Help them understand their responsibilities. Everyone needs general awareness however those with specific responsibility need training at a more advanced level.