A TALE OF BS 7799-2 CERTIFICATION

A personal account by Dr. David Brewer, Chairman Gamma Secure Systems Limited

The objective of this paper is to tell the story of Gamma's BS 7799-2 certification in the hope that other organisations, particularly small ones such as Gamma, may benefit from our experiences.

My story starts about two years ago when Gamma decided it should extend the scope of its internal control system (ICS) to conform with BS 7799-2:2000. I remember the date precisely: it was 12th September 2002. I was chairing an internal management review meeting, and we were discussing a recently completed review of our security procedures. Our agreed constraint was to complete ICS transition from ISO 9001:1994 to ISO 9001:2000 first, which we subsequently achieved in November 2002.

Information security is not something that is new to Gamma. It is in fact our livelihood, as we are information security consultants; it has been an integral part of our ICS ever since the company's inception in 1988, and we are some of the principal contributors to the development of the standard. However, any hope of going for an autumn certification in 2003 was dashed with the advent of a number of unexpected overseas commitments that took me, in particular, out of the UK for months at a time. The first opportunity we had to re-establish our goal was 5th March 2004. I will now recount the events from that day to the award of our BS 7799-2 certificate.

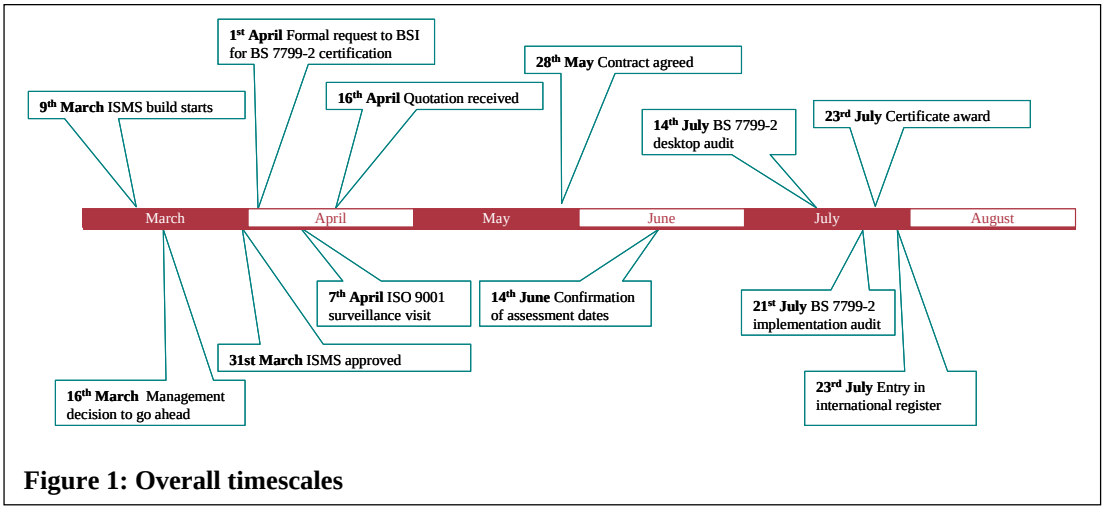

Figure 1: Overall timescales

THE DECISION

At lunch on 5th March, my co-director, Mike Nash, asked me how long it would take to extend our already web-technology based management system to cover BS 7799-2. I suspected a few days, but before making any seemingly outrageous promises or commitments, I replied that I would see how long it would take to complete the SOA.

I would not normally start with the SOA, but as a founder director of the company, I have an intimate knowledge of the company's risks and risk treatment. I also have an intimate knowledge of our management system and existing controls. As one of the authors of BS 7799-2, I also knew that there are 127 controls listed in BS 7799-2 and at one minute each, that would take 2 hours. It is arguably one of the most time consuming activities in building an ISMS. Of course, the Skeleton ISMS manual that Gamma uses to create its customers' ISMS [1] would give me a head start.

I started work on 9th March, spending the first part of the morning integrating the Skeleton ISMS manual into a development copy of Gamma's existing management system. By close of play the next day the SOA was ready for formal review, complete apart from some hyperlinks that would have to be added later. It is important to realise that as a security consultancy practicing what it preaches, all the security controls were in place and documented. In completing the SOA, all I needed to know was what they were and where were they documented. I had averaged about 6 minutes per control.

Mike reviewed the SOA on 12th March, and with a few minor modifications judged it fit for purpose. The Skeleton had done its job, and in fact I had

broken the back of developing the build of Gamma's ISMS.

Our next ISO 9001 surveillance visit was due on 7th April. Mike was particularly keen on having our ISMS ready by then, and by ready he meant: complete, approved and operational. Having completed the SOA, neither Mike nor I had any reservations about meeting this objective. We formally made the resource commitment in a Management System Review Meeting on 16th March and set 2nd April as the target date for completion.

COMPLETING THE ISMS

Now that I had management approval, I could complete and authorise the change requests, enter the project plan into the "To-Do-List", and integrate the SOA into the development system proper. I started on 22nd March. All the changes were complete and approved by 31st March. Total build effort, including the SOA work was just six days – testimony to all the hard work over the years by our staff in establishing the initial Quality Management System in 1994, our recent work in converting it to a web-technology based system, and the development of the ISMS Skeleton Manual. A description of the complete ICS is given in [2].

CONTRACT NEGOTIATION

The next step was to negotiate the certification contract. Our goal was one management system, one audit, but two standards – ISO 9001 and BS 7799-2. I contacted our certification body, BSI, by e-mail on 1st April. We showed off our new management system during our ISO 9001 surveillance visit and secured our assessor's assistance in gaining a positive response. We received a quotation on 16th April but it assumed that we were just going for BS 7799-2 certification and did not take account of our ISO 9001 certification. We redrew BSI's attention to our specification (one management system, one audit, but two standards). BSI apologised profusely for their misunderstanding and we received an acceptable quotation on 28th May, which we agreed by return.

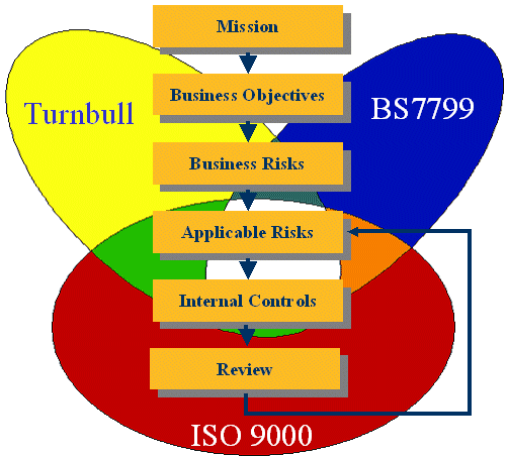

Figure 2 - ISMS and QMS are just parts of the overall internal control system

We were now in a position to set the dates for the assessments. The earliest BSI could offer was 14th and 21st July. We acceded to their suggestion.

1st ASSESSMENT VISIT

It might have seemed a long time ago that I had first contacted BSI, 3½ months to be exact, but the day finally arrived. It got off to an amusing start when BSI rang to say that our new assessor was lost and could not find the office. Mike phoned him and gave him directions. Soon we were all having a warm cup of coffee together and the half-day desktop audit was underway. It transpired that our assessor had been given the wrong address by the person in BSI responsible for scheduling audits!

First impressions

My first impression was that I was dealing with an assessor that was extremely competent in both BS 7799-2 and ISO 9001. This was starting to put the realisation of our goal of "one audit two standards" comfortably within our grasp.

The purpose of the desktop audit is to confirm that the management system, as documented, conforms to the standard. My job was to guide the assessor through the management system. Being an integrated management system we would naturally flick from one standard to another as we navigated through it.

Just a click away

Being a web-technology based system, navigation through the ISMS manual is by clicking on hypertext links. In one particular sequence, I showed how internal audit observations, management system review actions, To-Do-List entries, change request forms and document control records all fitted together. In the space of a few minutes I had demonstrated how our management system had meet about 50% of the BS 7799-2 requirements. The assessor asked me another question. I clicked the hyperlink. The answer appeared in a footnote window (see [1]). Mike noticed the assessor smile with glee.

In fact, virtually everything we looked at was immediately accessible on my computer screen.

The only paper file we looked was my correspondence file with BSI concerning our original ISO 9001:1994 certification.

Risk assessment

We looked in detail at the risk assessment. As the management system covers the whole of our internal control system, the risk assessment follows the UK Audit Practice Board [3] guidance and starts with the company mission statement and business objectives (see Figure 2). It is driven by an analysis of events and impacts (see [4]), from which we *derive* the assets and threats. Vulnerabilities are dealt with on the fly in producing the risk treatment plans. This approach did not come as a surprise to our assessor. He told me that several of his clients had discovered that it was best to start with events and impacts, and he clearly understood that it made good business sense to do so.

Documentation

In looking at our Management System Policy (which is our implementation of the BS 7799-2 requirement to have an ISMS policy), our assessor noted our policy statement on documentation, where we state the rules for what must be documented and for what need not. This led to an interesting conversation about culture, where the assessor pointed out that in some organisations procedures that must be followed by many people are not documented, but everyone still knows what to do. I pointed out that one had at least to document that fact, e.g. in the SOA, that the procedure is part of the organisation's culture, but that it is auditable. "*Yes*", said our assessor, "*ask a selection of people what the procedure is, and if they all give the right answer there is good evidence to show that they're all following it.*"

Why do things that way?

In response to another question Mike answered, "*For historical reasons*." That clearly was the right response. The real question the assessor was asking was "*Do you know why you do it that way?*"

The SOA

After about two hours we had had a good look at the risk assessment and all the management processes. All that remained was the SOA.

Once I had demonstrated how it worked, with its backwards hyperlinks to the applicable risk treatment plans and policy statements, and forward links to documented procedures (see [1], [2]), we quickly went through it from beginning to end. The assessor was particularly interested in the controls that we had marked as being non-applicable. For each he asked a variety of quite searching questions, and was satisfied with our answers.

Clearly, our assessor expected some controls to be there without exception, such as business continuity, and indeed they were.

Finally we looked at a selection of procedures. In doing this, I was able to show him the change control and approval history, and a variety of further cross references to audit and management system review actions.

Conclusion

The desktop audit was over by 12:30. We had looked at the entire management system for conformity with the standard and, of course in passing, had unearthed a lot of the implementation evidence (really the subject of the second audit), such as internal audits and management system reviews.

Of course, not all desktop audits would proceed this smoothly. We understood BS 7799-2 thoroughly, which meant the assessor had little explaining to do, and our management procedures were well established, accurately documented, and already certified for quality management.

2nd ASSESSMENT VISIT

The second assessment visit was held one week later. It started promptly at 09:15 (everyone knew where to go this time), and naturally concentrated on the SOA. This was familiar ground to all of us and the time passed quickly.

Stay calm

This assessment also got off to an amusing start, when the assessor started by asking for a print out of the SOA. That did not prove straightforward. The desktop from which I was running the management system seemed to be able to print anything I asked of it except the management system – I still don't know why; later I was unable to reproduce the problem. Eventually I decided to generate the print from my laptop. After what seemed like ten minutes but was probably only a few seconds the printer whirred away and delivered the right output. "*Why do you want a print out of an electronic document?*", I enquired with a smile. "*Ah!*", replied the assessor, sensing the funny side of his request. Clearly, printing out electronic documents was not the sort of activity we engaged in regularly.

In fact, as we completed examining each topic, he crossed it off on his printed copy, thus giving him his reminder and evidence that every section had been covered.

Version number

His next question was "*What is the version number of the SOA?*" BSI wants this for the certificate, which is a nuisance, as it implies that the SOA needs to be a single configuration item, and in Gamma's management system each web page is a separate configuration item. Coincidentally, all bar the index page had identical version numbers, so we settled on that.

In the long term, I am going to have to find some more elegant solution that permits continuous review and improvement, but has a fixed version number to keep the certification happy.

Audit process

Starting with the section on security policy, the assessor would select a number of controls, ask us various questions about our implementation of them, then move on to the next section of the SOA.

I tended to answer the questions by reinforcing what was written in the SOA and using the hyperlinks to provide the supporting evidence. Remember, this was an implementation audit and therefore the assessor looking for evidence that the controls, as well as other management system components were being implemented.

Figure 3 – Gamma's ISO 9001 and BS 7799-2 certificates

Records

Often the assessor would ask what records I kept. The answer to that question, in the context of the management processes, was straightforward as they are all, bar the incident log, in the electronic manual (and therefore just a click away). The assessor's more revealing questions, to my mind, concerned the controls. For example, he asked, looking at the controls concerned with access control, "*What records do you keep?*" My reply was to say "*Here is the policy*", clicking on the hyperlink that revealed the applicable access control policy, "*and the evidence of its implementation is in that computer*", pointing at my laptop. "*Let's have a look.*" I was taught a long time ago that access control in a computer is governed by what is its internal tables, not what a manager says that it ought to be – so the record is what is in the computer. I gave similar responses to his questions concerning antivirus and firewall logs.

It was the traditional audit approach. The assessor would ask seemingly innocent questions about how the technology worked, e.g. "live update", and once satisfied that I really did know the answer, he would move on to another topic. Exactly the same as in an ISO 9001 audit.

A comment that I would make at this stage concerns the advice given in BS 7799-2 in Annex B on routine checking. It's not a mandatory requirement, but it is something I practice regularly: know what your policies are and regularly check that they are enforced by the computer.

Metrics

After a most pleasant lunch with our assessor discussing practical problems interpreting BS 7799, we were on the downhill run to completion of the audit with just three sections of the SOA to go. The assessor had confirmed that he had seen how we had implemented many other BS 7799-2 requirements during the previous visit and during the course of the day. Eventually we reached the last section on the SOA. We dwelt a little while on the legal section as we had identified a number of applicable laws. The interesting discussion however, concerned compliance, where we entered a useful debate about metrics. Metrics is a requirement for ISO 9001 but not for BS 7799-2. I am, however, working on them using our "time" theory [4] as a guide.

The final hour

We completed the SOA at about 14:30. The assessor spent the next hour completing his report, which he then presented to Mike and me in the customary manner. It was a positive report, recommending unqualified certification, there being no non-conformities to attend to. Having dealt with that, we then spent the next twenty minutes talking about some practical issues, which Mike and I found significantly more interesting, such as when do we get the certificate? and can BSI help us with press releases?, as well as some further very useful feedback on BS 7799 practicalities from an assessor's viewpoint.

CERTIFICATE AWARD

The promise was two weeks, a significant improvement on the early days of BS 7799 certification when we were told it could have taken three months. Registration was in fact two days later on 23rd July. BSI took care of our entry in the International Register and in fact I saw that before the certificate arrived in the post. Well done everyone.

OVERALL CONCLUSION

Importance of internal control

I am confident that the key to our success lies in giving pride of place to the internal control system. Its purpose is to assist Mike and I in managing our business, to assure the quality of our work and to manage our business risks. We use it every day. Internal audits and management system reviews are part and parcel of our belief and practice of sound management techniques, such as the Deming cycle (Plan-Do-Check-Act). It is not something that we resurrect and polish up just before an audit, only then to put away and forget about until next time.

Power of web technology

Our management system is easy to use and maintain, as are all the internal controls. There is no bureaucracy. Nothing gets in the way of the business. Both internal and external audits are very fast, with everything being just a "click away".

Could it have been done faster?

Three years ago, I negotiated the BS 7799-2 certification with BSI for Vodafone Information Systems in Rattingen, Germany. From initial contact to presentation of the certification at the 2001 Cebit exhibition took 42 days, so the answer is possibly yes. If Gamma had been content with treating ISO 9001 and BS 7799-2 as separate management systems, we could have possibly saved six weeks, but then we would not have met our objective of "one management system, one audit, two standards".

Was it all worth it?

As an author of the standard, I was adamant in the early days to ensure that large organisations did not enforce compliance with the standard on their smaller suppliers without having first gained the standard for themselves. I and my colleagues in BDD/2 (the BSI committee responsible at that time for BS 7799-2) lobbied vehemently for that, and I was pleased when the head of the UK Civil Service instructed all UK government departments to have BS 7799 in place by the end of 2000. Leadership from the top. I always mention that in the various seminars and training courses I have given on the standard across the world. I reinforce my remarks by pointing out the requirements for management commitment and approval in the standard. It makes a great deal of sense to follow the same practice, and have own our ISMS and to be an integral part of its management and administration.

Some people will say that BS 7799 certification for an organisation the size of Gamma is overkill. My reply is always to ask how you can trust an advisor on BS 7799 who cannot show how he or she meets its requirements for themselves. It one thing to have helped to write the standard to have helped others to implement it; but quite another to use, maintain and improve your very own ISMS on a daily basis. In providing consultancy services we can truly say that "*we have been there, done that, wrote the book…*" In short, we have our very own certification tales to tell.

REFERENCES

[1] "Fast Track ISMS Certification", Brewer, D.F.C., List, W., August 2004, www.gammassl.co.uk/topics/ics/FTISMS.pdf

[2] "A description of Gamma's internal control system", www.gammassl.co.uk/topics/ics/gamma.html

[3] "Briefing paper - Providing Assurance on the effectiveness of Internal Control" issued by the Audit Practices Board July 2001, www.apb.org.uk/ Copies are also available from ABG Professional Information

[4] "Measuring the effectiveness of an internal control system", Brewer, D.F.C., List, W., March 2004, www.gammassl.co.uk/topics/time/RTPs.htmlT