

FAST TRACK ISMS CERTIFICATION

by Dr. David Brewer and William List, CA, Hon FBCS, CITP

At a press conference on 29 April 2004 there were gasps of awe from the audience as we announced that four clients of ours based in that country had achieved BS 7799-2 [1] *attestation*¹ in less than four months each from a standing start.

The senior executives of the four organisations shared their experiences with the invited audience, press and television, and left them in no doubt that:

- Fast track ISMS certification is a reality, made possible by the diligent application of the chosen methodology.
- The process had empowered them to take ownership of information assurance and make information security decisions by themselves in support of their organisations business objectives.
- Information assurance is an integral part of corporate governance.

The objective of this paper is to share our experiences in using that methodology.

We begin by highlighting and discussing the most salient features of the de facto international Information Security Management System (ISMS) standard, BS 7799-2. As authors of this standard, we then review the challenges that we and others have experienced in its implementation. This led us to devise the methodology that we now reveal. We then examine the methodology in detail, looking particularly at how it is constructed and how the various components work and fit together. We then describe our experiences of using this methodology on a variety of projects worldwide, and thus present our results and conclusions.

BACKGROUND AND MOTIVATION

Imperatives of BS 7799-2

There are five very important points to remember about BS 7799-2:2002.

¹ *Attestation* is a French word meaning the equivalent of international certification while the certification body is still in the process of gaining ISMS accreditation. The certification body in this case was an experienced and accredited ISO 9000 certification body, in the process of extending its scope of accreditation to cover BS 7799-2.

1. Management

BS 7799-2:2002 is a *management* standard. It is a tool for executive directors (and senior managers) and requires their leadership, involvement and commitment.

2. Internal control

BS 7799-2:2002 is a specification for building, operating, maintaining and improving an ISMS. However, an ISMS is just *part* of an organisation's internal control system. Management establish an internal control system to marshal their organisation's resources to achieve their business objectives and manage the associated risks. An ISMS can be regarded as that part of the internal control system where information security/assurance² is a concern.

3. Business risk

The selection of information assurance controls is predominantly determined by risk assessment. This assessment must be performed in the context of meeting the organisation's business objectives, a fact that BS 7799-2:2002 consistently refers to in discussing risk management decisions.

The selection of information assurance controls may also be determined by policy. Such policy is often set by some higher authority, which has itself performed a risk assessment, the results of which it expresses as policy that it and its subordinates must adhere to. An example would be a government department, which is bound by the national rules for protecting classified information. Thus, in the Statement of Applicability (SOA) an applicable control may refer back to a statement in a risk assessment or a policy.

4. Deming cycle

As part of an internal control system, an ISMS operates on the Deming cycle, also known as the Plan-Do-Check-Act (PDCA) cycle. Plan what you want to do, do it, check that it is working, and take appropriate action if not.

The principal components of BS 7799-2, associated with each phase of the PDCA cycle, are shown in Figure 1.

² The term information *assurance* is gradually taking over from the term information security, to place greater emphasis on integrity (i.e. that information must be sufficiently right for the purpose for which it is used at the time that it is used).

5. A journey not a destination

An important corollary of the PDCA model is that at any point in time there may be corrective/preventive actions and improvements that have been identified but have yet to be implemented. There may also be incidents that are in the process of being dealt with. It is the task of the internal control system (and therefore the ISMS) to manage these activities.

It is therefore important to realise that an ISMS is a journey and not a destination. An analogy is the “death star” in the movie Star Wars, the Return of the Jedi. The death star appears to be unfinished, but it is nonetheless fully operational. Thus an internal control system/ ISMS can have tasks on its To-Do-List, which provided they do not render the organisation inoperative, do not imply that the internal control system/ ISMS is itself defective. This conclusion is reflected in the rather convoluted definition of non-conformity given in EA7/03 [2], which defines the rules for certification bodies wishing to assess an organisation’s ISMS:

The absence of, or the failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the security policy and objectives of the organisation.

Challenges of ISMS implementation

What is ISO/IEC 17799?

ISO/IEC 17799:2000 [3] is a companion document to BS7799-2; indeed it was originally published as BS 7799 Part 1. It is a code of practice of good security things to do.

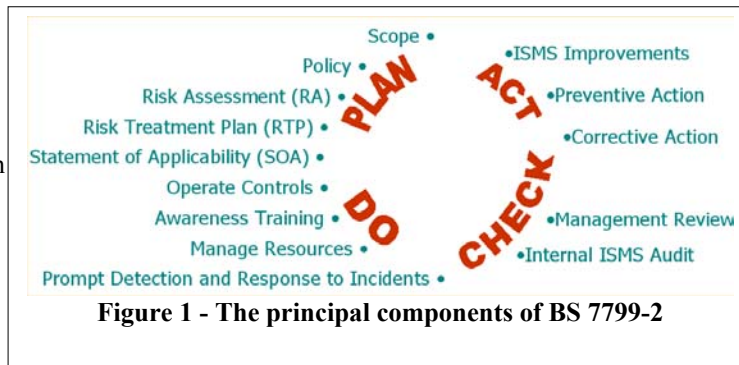
An analogy may help. Suppose you were considering throwing a party for the first time. What do you do? The management system specification (i.e. BS 7799-2) tells you everything you need to do to make your party a success. Having made your initial plans, you might then go to a supermarket to see what fine foods and gifts you might buy for your party. As you research the supermarket, three things are certain:

- You will only buy what you need. (In information assurance terms, that is what is

demanded by policy and what you require as a result of your risk analysis.)

- You will not buy everything on offer in the supermarket (in other words some controls in ISO/IEC 17799 might not be applicable)
- You may buy some items from another shop (i.e., you may require controls that are not listed in ISO/IEC 17799).

This third point is very important. It underlies the fact that ISO/IEC 17799 is just a laundry list, and if it is unsuitable for your purpose, you can look elsewhere. Nevertheless, ISO/IEC 17799 is very comprehensive and provides good general high level



security guidance under 10 major headings (see Figure 2). Note also that the scope of the standard is information security/assurance; it is not restricted to just information technology.

There is too much to document

Anyone who has implemented an ISO 9001 quality management system (QMS) [4] will realise that there is a lot of documentation to produce, a lot of records to keep, and seemingly a lot of bureaucracy that has no value to the organisation apart from helping it to get a “tick in the box”.

There is seemingly just as much documentation involved in BS 7799-2, and the SOA is particularly tedious to create. The need to document the risk assessment and risk treatment plans can be arduous, and appears to encourage the use of sophisticated IT risk assessment tools, the output of some of which is barely comprehensible. *Smile.com* made this point most emphatically at the first ever “7799 Goes Global conference” (London, September 2002), sharing its insistence that its consultants used a paper-based approach so that senior management could understand the results.

It takes too long

A consequence of the seemingly high volumes of documentation and records required is the resource and time necessary to produce them, particularly if the chosen resources have other important jobs to do. Durations of one or two years are often quoted. Nevertheless, both BS 7799-2 and ISO 9001 place demands on ensuring the availability of resources.

Engaging the Board

Quite often it is the IT department that is tasked with looking into BS 7799-2. How do they engage with the Board in order to ensure that the risk assessments are carried out in the context of the business?

When we have asked the CEO, or other main board director “what are your information assets”, the answer is often a blank stare or directions to the IT department.

Our question “what are your threats” has met with the same response, and we rarely dared to ask, “what are your vulnerabilities”.

Both BS 7799-2 and ISO 9001 place demands on management commitment. How can management be committed if it plays no role in the process of developing and operating the ISMS?

Is the ISMS really the domain of the IT department?

ISO 9001 does not currently have a requirement for risk analysis, although we understand that it may well have in the future. If it did, many organisations would no doubt identify that the major quality risk lay in the production department, where it is usual for the QMS to reside. Other departments, such as finance and sales/marketing by comparison present less of a quality risk. However, only part of the information assurance risk lies with the IT department. The information risk applies to every department. The extent to which IT is involved will depend on the reliance the organisation places on its IT systems. What is clear is that not all the information assurance risk lies within IT.

Does BS 7799-2, or for that matter ISO/IEC 17799, really address the business risk requirement?

BS 7799-2 says that you must link information security with business objectives, but offers no guidance on how you might do it.

ISO/IEC 17799, in common with other information security standards (e.g. the Common Criteria, ISO/IEC 15408 [5]), certainly at first view concentrates on platform security. If you secure the IT platform, does this mean that information assurance is guaranteed? The answer unfortunately is no. A hardened operating system, firewalls, anti-

virus, network intrusion detection and other platform level security technology does not directly deal with ensuring that, for example, financial data and the presentation of accounts are correct. Nor does it help with addressing risks such as:

- One of my aircraft has broken down in the Indian Ocean
- Our mark-to-market valuation (for derivatives) is incorrect
- The automated trains in our warehouse have just crashed into each other

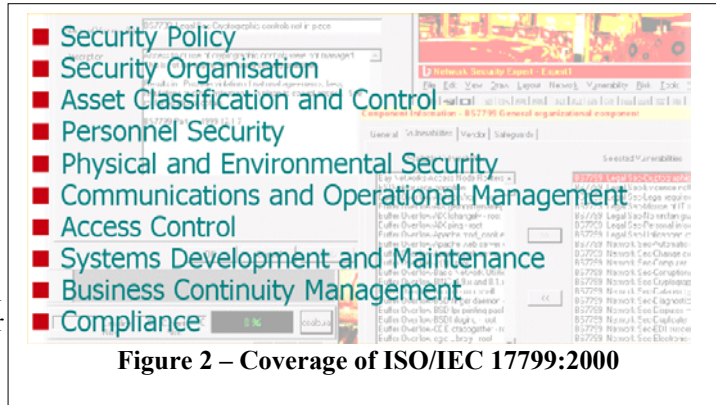


Figure 2 – Coverage of ISO/IEC 17799:2000

yet all are clearly concerned with information, and indeed information technology.

Training, awareness and competence

Both BS 7799-2 and ISO 9001 place demands on training and the need to appraise and record the effectiveness of the training. This is often regarded as a serious overhead for small and medium sized enterprises (SMEs). BS 7799-2 places further demands on security awareness training and competence.

Why bother with certification?

Certification is, of course, necessary if you wish third party endorsement of the fact that your ISMS complies with BS 7799-2, just as you would do if you wished similar endorsement that your QMS complies with ISO 9001:2000.

For readers unfamiliar with ISMS certification it is very similar to QMS certification. The rules in this case, however, are laid down in EA7/03. There will be an initial audit performed in two parts, followed by a series of surveillance audits, usually at 6 month intervals, and a tri-annual reassessment. The first part of the initial audit is sometimes called a “desktop” audit, as its purpose is to determine technical compliance of the ISMS documentation with BS 7799-2. The second part is sometimes referred to as an “implementation” audit, as its purpose is to discover whether the organisation practices what it preaches.

Assessors will focus on the management system aspects of BS 7799-2 and then look at the information assurance controls. If there are challenges associated with assessment, it seems either to be the fear of failure, or the time and expense of the assessment, particularly if the latter appears disproportionate compared to the effort that is expended internally on audit.

There has to be a better way

Thus, in summary, the challenges are:

- The engagement of the Board in an issue that many incorrectly regard as being the domain of the IT department
- The difficulty in ensuring that the risk assessment adequately reflects the business objectives of the organisation
- The tediousness of creating the SOA, and the arduousness of documenting the risk assessment and risk treatment plans
- The apparent need for volumes of documentation and records
- The procedures necessary for internal audit and management review, training, awareness and competence
- The costs, resources and time involved in setting up and administering the ISMS
- The costs, resources and time involved in certification.

We, as well as many others, believe that the goal of ISMS certification is worthwhile. There just has to be a better way of achieving it.

METHODOLOGY

Overture

The need to address these challenges first came when one of us was tasked with upgrading his company's ISO 9001:1994 QMS to comply with ISO 9001:2000. Early on in this process, that company (Gamma) took the decision to revise its internal control system based on the advice given by the Audit Practice Board [6], produced to assist in the application of the Turnbull report [7], and to implement that new control system using electronic documentation. Gamma finally concluded that this could best be done using web technology (hypertext) and should include not only the procedures (Plan and Do) but also all the records associated with the control system (Check and Act).

Starting with the company's mission statement, Gamma articulated its business objectives and business risks, and mapped these onto its extant internal controls, originally established not only to satisfy the requirements of ISO 9001:1994 but also to deal with the financial and security concerns of the company. Both authors were involved in this process, the one masterminding the design and implementation, the other providing invaluable advice and guidance. One of our particular

conclusions that resulted from this exercise was that the ISMS and QMS were integral components of the overall internal control system, as illustrated in Figure 3.

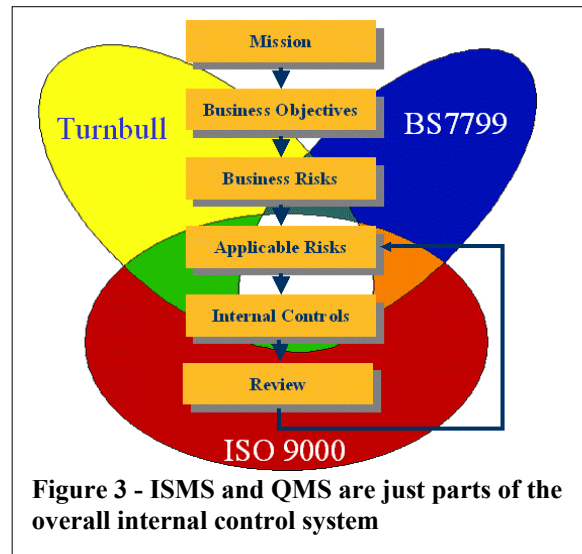


Figure 3 - ISMS and QMS are just parts of the overall internal control system

In parallel, one of us undertook an assignment to assist a UK company to develop an ISMS. The person who commissioned the assignment was none other than that company's managing director. Through him we learnt the easy way to engage the Board.

The fast track methodology essentially fell out of these two projects. The one gave rise to the concept of using an electronically documented internal control system or, just in the context of BS 7799-2, an ISMS. The other gave rise to a unique risk assessment approach, which is innovative merely in the sense that it starts with the management and engages with them in their own business language.

The need to implement ISMS systems for four customers in parallel was a powerful driver to convert these thoughts and conclusions into a reusable methodology. We concluded that *empowerment* and a *robust, repeatable methodology* were the names of the game.

The primary ingredients of the methodology were:

- A role model defining the responsibilities and interactions of all the actors that would be involved with the ISMS
- An electronically documented "Skeleton" ISMS manual, covering *all* BS 7799-2 requirements
- A business-led approach to risk assessment and the production of risk treatment plans
- Classroom and on-the-job training

Fast Track ISMS Certification

- Various quality assurance activities
- Not least, a committed and enthusiastic client to work with.

The last ingredient has always been a given. In the next section we review and discuss the other ingredients.

The vital recipe

A role model

BS 7799-2 gives very scant advice on the roles involved in producing and administering an ISMS. In fact it only identifies one role, i.e., that of internal ISMS auditor.

We consider that seven distinct roles are necessary to build a successful ISMS, defined as follows:

- *Information Security Forum (ISF)*. This takes its rise from a term used in ISO/IEC 17799 and forms the senior management team that owns the ISMS. It approves policy and takes responsibility for accepting residual information assurance risk. It is also responsible for conducting the management system reviews defined in the standard.
- *ISMS administrator*. These are the people who take day-to-day responsibility for administering the ISMS. They would be the people, for example, who construct and maintain the ISMS manual described below.
- *Internal ISMS auditor*. These are the people who carry out the internal ISMS audit role identified in the standard.
- *ISMS trainer*. These are the people who carry out, or are responsible for ensuring that the training, awareness and competence requirements defined in the standard are met.
- *ISMS advisor*. These are the people who provide advice to all the abovementioned roles.
- *Certification auditor*. These are the people employed by a certification body who perform assessments of compliance against the standard.
- *Policy maker*. These are the people external to the ISMS who define policies, laws and regulations with which the ISMS must comply.

As in any role model, an *actor* (e.g. a person or some other entity) may play several roles and several actors may play any given role. In Gamma for example, which has two executive directors,

both are members of the ISF and each play the roles of internal ISMS auditor, ISMS trainer and ISMS advisor, and one in addition plays the role of ISMS administrator. The roles of certification auditor and policy maker are played by people and organisations external to the company.

Skeleton ISMS manual

The Skeleton ISMS manual is simply a documentation aid, but as such it is extremely powerful as it is designed to address every single requirement in BS 7799-2. The desktop audits that have been performed using the Skeleton (see [later](#)) are testimony to the success of its design.

It is an html document and is therefore read using a browser and modified using an html editor. The design uses a simple frames layout, with a navigation bar to the left, a banner frame, the main window and a footnotes window (see Figure 4). Clicking on a hyperlink will replace the content of the main window, open up a new window, or reveal explanatory information in the footnotes window. In this third case, once the information has been read, it can be cleared using the lowermost button in the navigation bar.

As illustrated in Figure 4, there *are* parts for the organisation to complete, but the structure and standard text are already present.

The Skeleton contains:

- Pages associated with the whole of the PDCA cycle.
- A built-in facility for document control, which is a particular requirement of BS 7799-2 (and indeed ISO 9001). It operates at the level of each page. The ISMS also has a version number as a whole.
- Space to define the scope of the ISMS and the information/business context in which it is used.
- A built-in near completed prototype ISMS policy that covers all the requirements of BS 7799-2. All that needs to be done to complete it is to define the ISF, agree its terms of reference and confirm (or amend accordingly) the detailed wording of the policy statements. It should be noted that some of these policy statements are used to simplify the SOA and the two are hyperlinked together.
- Provision for carrying out the risk assessment and producing the risk treatment plans (RTPs) in accordance with our particular approach (see below). There are eight standard RTPs, which are built into the Skeleton, and a provision for the user to add others. To assist in achieving

Fast Track ISMS Certification

compliance, there are ready-made *asset, threat* and *impact* lists. Vulnerabilities are addressed during the process of fleshing out the RTPs.

The management review procedure is defined and there is a ready-made schedule.

The screenshot shows the 'ISMS Manual' home page. Callouts include: 'Covers every requirement of BS7799-2:2002' pointing to the title; 'Built in document control facility' pointing to the top navigation; 'Parts for you to complete' pointing to the 'Purpose' and 'Contents' sections; 'Footnote area' pointing to the bottom left; and 'Head start for record keeping' pointing to a note about data loss.

Figure 4 - Skeleton ISMS manual home page

- Built-in processes to address the Act requirements for corrective/preventive action and improvement.
- A To-Do-List and associated procedures.
- A compliance index, which takes every requirement in BS 7799-2 and hyperlinks it to the primary page, which addresses that requirement.

Risk treatment plans

Our risk assessment approach starts with the *events* and the *impacts*. The event is something that causes the impact. In business terms, the impacts

- A virtually complete SOA, which is backwards linked to relevant policy statements and the standard risk assessment events, see Figure 5. Each of the 127 controls in the SOA is also linked to five skeleton handbooks/manuals (staff handbook, managers' handbook, operations manual, IT development manual and business continuity plan) as appropriate. These skeleton handbooks/manuals provide a head start in producing the necessary procedures. If the procedures already exist, just copy them in. To complete the SOA, all that needs to be done is to link the controls to any user defined RTPs and mark as non-applicable those BS 7799-2 controls, which are not going to be implemented based on management decisions following from the results of the risk assessment.
- A facility for inclusion of the training and awareness programme.
- A built-in internal ISMS audit proforma and checklist, which ensures compliance of internal ISMS audits to the requirements of BS 7799-2. The internal audit procedure is defined and there is a ready-made schedule.
- A built-in management system review checklist for use by the meeting secretary. Completion of the checklist will ensure that all inputs, discussion topics and outputs, required by BS 7799-2 are addressed at the meeting.

that seem to capture the interest of senior executives include:

- Adverse press coverage
- Customer dissatisfaction
- Inability to carry out some or all of the organisation's business
- Loss of revenue
- Unanticipated costs
- Court action against an employee or the organisation itself.

Starting with these, we then ask what events might cause them. In practice, we have identified eight standard events, which we believe are common to most, if not all, organisations, to which we invite the ISF to add those that are the special concerns of the organisation itself. The events that we mentioned in the earlier section entitled "[Does BS 7799-2 ... really address the business risk requirement?](#)" are indeed examples of such "user defined" events. The eight standard events are:

- Theft
- Acts of God, vandalism and terrorism
- Fraud
- IT failure
- Hacking
- Denial of service

- Disclosure
- Legal.

In developing an RTP, the idea is to ensure that wherever possible the *occurrence of the event can be detected in sufficient time* to do something positive about it before the impact occurs.

In some cases, it may be possible to prevent the event or detect it whilst it is happening and thereby prevent any further activity that may lead to an impact. Such are the *preventive* controls. Having considered these, it is then necessary to consider the *detective* controls, if for no other reason than to appreciate that in practice the preventive controls may fail. The objective of the detective controls is to identify when some event, or events have occurred that could lead to a materialisation of the impact, and invoke appropriate actions to arrest (or mitigate) the situation. Finally, it is necessary to consider the *reactive* controls, which identify that the impact has occurred (e.g. because of a failure of the detective controls) and invoke appropriate actions to recover (or mitigate) the situation. The process terminates when management decide that any residual risk is acceptable.

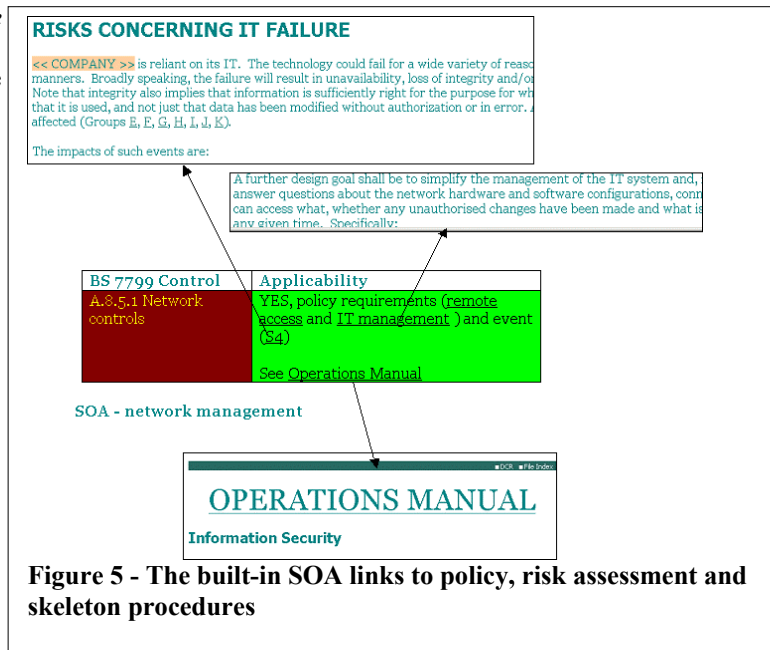
A procedure for constructing RTPs is given in our paper on measuring the effectiveness of internal control systems [8], which also details the theory and practice concerning time to detect and time to react.

Classroom and on-the-job training

Empowerment can only be achieved if the programme facilitates knowledge transfer to the actors that will play the various roles defined earlier. One way to do this is through formal classroom training, followed by on-the-job training and supervision. We use a two day course covering both BS 7799-2 and ISO/IEC 17799, which teaches the trainees how to implement and administer an ISMS. It consists of a variety of lectures interspersed with syndicate exercises, and already includes practice on developing RTPs. We tailored this course for our new purposes by incorporating training on the Skeleton, and creating a one day session on internal ISMS audit. Again split between lectures and practice, this session addressed both compliance and substantive audit techniques.

Quality assurance

The final ingredient of our methodology also concerns empowerment and is designed to ensure the programme stays on course and to impart further



confidence in the ability to discharge their new responsibilities to the actors involved.

Activities usually include:

- Carrying out quality assurance reviews of the completed ISMS manual
- Assisting the internal ISMS auditors.

FAST TRACK IN PRACTICE

Introduction

In this section we share our experiences in applying the methodology. The projects concerned are varied and were carried out both at home and overseas.

Populating the role model

It is all well and good having a role model. It works very well in practice. However, it is very important to populate it with the actual actors that will play those roles early on in the ISMS development programme.

In many organisations these actors will already exist and may already be playing similar roles. All will have Boards and senior management committees that can perform the ISF role. Many others will have an existing internal audit function, and even perhaps a computer audit function, that can play the role of internal ISMS auditor.

Fast Track ISMS Certification

Without establishing an ISF the project cannot begin, as there is no approval forum. Ideally all the actors should be in place at the start and all should be trained together. Late identification of actors may cause additional training costs and reworking of the good work already done by others.

Engaging the Board

As a means of engaging the Board, the event-impact approach works extremely well. The trick lies in starting with the events and impacts that are the greatest concern to the Board members. Invariably, these are not any of the standard eight but are of the user-defined variety (such as “one of my aircraft has broken down ...”).

Because the subject is close to their heart, documenting the RTP then becomes somewhat akin to writing down the story of their “worst nightmare”, albeit at each twist of the story proudly showing how their controls save the day. It is possible that they will find some of their controls wanting, but the flaws we have been shown have been extremely subtle, and it is easy to see how they might have been missed before the application of this approach. The discovery of such flaws is, of course, an early win for the method and significantly increases the confidence of those using it. The Board/ISF sees immediately that the approach deals with the business requirement and is clearly not just the domain of the IT department.

Indeed, we have known for some time how to construct the scope statement so that it clearly describes what the organisation does. We have now learnt that the same can be done with the user-defined RTPs. In one case, for example, the first such RTP demonstrates why their project is superior to their competitors. This is magic for the sales/marketing members of the ISF.

After dealing with the user-defined RTPs, it appears to be a straightforward matter then to deal with the standard ones. Some of these are pretty well focussed towards IT, but this does present a problem even though some directors may be unfamiliar with the technical details. Of importance is that, by now, the different directors that comprise the ISF will have a good understanding of what each other’s risks are, and how they can assist each other. That adds up to good teamwork – another sign that the principle of empowerment is working.

Development time

The overall time from a standing start to *attestation*, as reported in the introduction, was

about four months (see Figure 6). We are finding similar times on other projects. Much of this time is actually spent on other activities and waiting on external events, in particular the availability of the certification body.

Indeed, even in the early stages when the activity is at

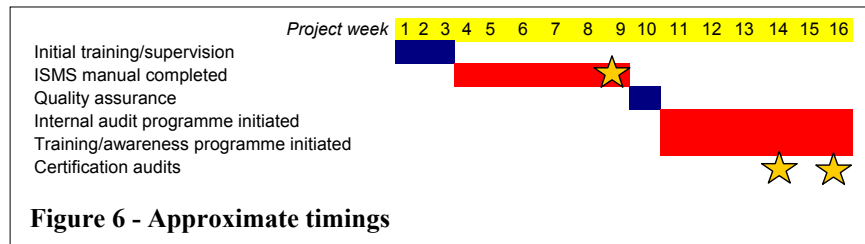


Figure 6 - Approximate timings

its most intense, the companies involved still have a business to run, and because of the seniority and specialisms of the people involved they are needed elsewhere.

Much of the time saved is due to the Skeleton. Indeed many of the ISMS advisors involved reported that they could not have carried out the task without the Skeleton.

Desktop audits

As part of our quality assurance activity it is usual for us to carry out a desktop audit as part of preparing our clients for the certification audits. The first time we did this, we performed the audit with the assistance of all the internal ISMS auditors, who we charged with taking a contemporaneous record of the proceedings. We diligently went through every clause and sub-clause in BS 7799-2 and, without the need for much prompting, the project team, led by a senior member of the ISF, was able to identify where in the ISMS manual the requirement was met. The process takes about two hours.

Speed of auditing

On that project, the certification body independently performed its own desktop audits and subsequently carried out the implementation audits. There were some minor observations.

Compared to the ISO 9001 audits that the certification body was used to, the speed of the BS 7799-2 audits is ultra quick. The certification body was able to do each audit in a day, averaging about 20-30% of the time taken for an ISO 9001 audit. We have achieved similar results with other certification bodies.

The rapidity is due to:

- The electronic form of the ISMS manual, where everything you need is just a “hyper click” away.
- The completeness of the ISMS manual, as it complies with all the BS 7799-2 requirements.

For Gamma’s internal control system, just about everything is electronic. Consequently the auditor is

able to follow the specification of the controls in the management system through to their application on a project with the click of a button.

Training and awareness

A final observation, which is no less important, concerns the increase in awareness of information assurance by everyone involved. The IT people have a far greater understanding of the business, its objectives and risks, and what role IT plays in meeting and managing them. Likewise, the “users” have a far greater understanding of the important role that information assurance and IT has to play in making the business successful.

The SOA may have a particular role to play here (as we believe any such laundry list would), as it acts as an eye-opener and as a checklist of possible controls that might otherwise be overlooked.

The testimony to the overall success of the approach, notwithstanding the speed at which it can be accomplished, is the empowerment of the senior users to decide what information assurance controls they need to fulfil their business objectives. In one particular case, one organisation was adamant at the outset that their security was completely adequate for their needs. Having completed the project to *attestation*, the senior user identified a number of additional controls that he wished to include by way of preventive measures and improvements. He proudly enumerated them at during the April conference. Truly this is empowerment.

CONCLUSIONS

1. The methodology works and leads to fast track certification.
2. The methodology engages the Board. It is able to address the business requirement and not just the IT.
3. It increases awareness of information assurance issues and controls. The SOA may have a particular role to play here, but it is the experience gained through involvement and participation in the programme that really leads to empowerment, with the result that:
 - Senior users are able to decide for themselves what information assurance controls they need to fulfil their business objectives
 - They, and the other actors involved, are able to discharge their respective duties without further assistance.

4. No doubt, as the information assurance community’s experience in dealing with different types of organisation grows, it will be better able to predict what the business issues are, and therefore what the user-defined events and impacts will be. We suspect that this body of knowledge may better enable IT people to ensure that IT is aligned with the business, as demanded by the IT Governance Institute [9].
5. The speed of the process owes much to the Skeleton ISMS manual. The tediousness of the completing the SOA is removed as most of it is already done, as is the case with other BS 7799-2 requirements. Nothing is forgotten as all the procedures (audit, management, reviews, document control and training, etc.) are provided for. Indeed, the completed manual is as near to a guarantee for a successful desktop audit as anyone could hope for. In completing the manual the client team concentrates on the business issues. Coupled with the use of hypertext technology, the electronic manual significantly:
 - Speeds up ISMS development
 - Simplifies ISMS administration
 - Streamlines certification
 - Reduces overall costs and timescales.
6. The methodology is directly extensible to other areas of internal control, such as ISO 9001 and traditional accounting practices and procedures. This is no accident. The ISMS methodology is in fact merely a subset of one that from the outset was designed to cover all aspects of internal control. Gamma’s internal control system already does this. ISMS and QMS are indeed an integral part of the overall internal control system.
7. Overall, the approach is a robust, repeatable methodology that delivers empowerment, and therefore meets the objectives that it was designed to meet.

Is there a better way? The answer may well lie in the implementation of this methodology.

ACKNOWLEDGMENTS

We wish to thank all our clients and colleagues who have been involved in one way or another in the development of our methodology and who have benefited from its application. We also wish to thank the Board of Gamma Secure Systems Limited for the funding to engage in this research work and for permission to publish it.

REFERENCES

- [1] “Information security management systems - Specification with guidance for use”, BS 7799-2:2002, British Standards Institution
- [2] “Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems”, February 2000, <http://www.european-accreditation.org/>
- [3] “Information technology - Code of practice for information security management”, ISO/IEC 17799:2000
- [4] “Quality management systems – Requirements”, BS EN ISO 9001:2000
- [5] “Common Criteria for Information Technology Security Evaluation”, ISO/IEC 15408:2000
- [6] “Briefing paper - Providing Assurance on the effectiveness of Internal Control” issued by the Audit Practices Board July 2001, <http://www.apb.org.uk/> Copies are also available from ABG Professional Information
- [7] “Internal Control, Guidance for directors on the Combined Code (The Turnbull Report)”, Institute of Chartered Accountants in England and Wales, see <http://www.icaew.co.uk/>
- [8] “Measuring the effectiveness of an internal control system”, Brewer, D.F.C., List, W., March 2004, <http://www.gammasl.co.uk/topics/time>
- [9] “Board Briefing on IT Governance”, IT Governance Institute, ISBN 1-893299-27-X, 2001, <http://www.itgi.org/>

About the authors

Dr. David Brewer is a founder director of Gamma. He has been involved in information security since he left university, and is an internationally recognised consultant in that subject. He was part of the team who created the ITSEC and the Common Criteria, and has worked for a wide range of government departments and commercial organisations both at home and abroad.



William List, CA,
hon FBCS CITP

Mr. William List, CA hon FBCS CITP, is the proprietor of W^m. List & Co. He has been involved in security and audit for some 40 years. He has been involved in the development of secure business applications and the development of various accounting and IT standards. He retired as a partner from KPMG. He is the chairman of the BCS security expert panel and a member of the ICAEW IT faculty committee

Both are currently part of the international team developing the 7799 family of standards, and are two of the driving forces behind the Part 2 ISMS standard. They provided training in implementing ISO/IEC 17799 and have assisted many clients to build ISMSs since 1998 in Europe, East Africa and the Fast East.



Dr. David Brewer