company of which I was CEO. When you're the CEO, and you're interested in it, you can make an ISMS happen – as I've proved a number of times. While this book will shorten the learning curve for other CEO's in my position, it's really aimed at the manager – often an IT or information security manager – who is charged with tackling an ISO 27001 implementation and who wants a sure route to a positive outcome. It identifies what the experience of many BS7799 implementations has taught me are the nine key steps to ISMS success. The lessons seem to apply in any organization, public sector or private, and anywhere in the world. They start with recognizing the challenges usually faced by anyone concerned to improve their organization's security posture.

The second biggest challenge that, in my experience, is faced by information security technologists everywhere in the world, is gaining – and keeping – the board's attention. The biggest challenge is gaining – and keeping – the *organization's interest* and *application* to the project. When boards do finally become aware of their need to act – and to act systematically and comprehensively – against information security threats, they become very interested in hearing from their information security specialists. They even develop an appetite for investing organizational dollars into hardware and software solutions, and to mandate the development of a new ISMS – or the tightening up of an existing one.

Of course, there's usually no better than a 50:50 chance that the 'solution' they want is anything more that the security flavour of the threat month – for instance, anti-virus solution sales increased when Nimda, Code Red and Melissa hit the headlines. Once deployed, any single solution is unlikely to alter the overall security posture of an organization by more than one degree, not least because any effective security solution requires an integrated combination of technology, procedure and user application. And integration of this order requires more than just a knee-jerk reaction to a current threat.

The even greater certainty is that most initiatives to develop an ISMS are likely to be seen as either a current management 'fad' or, even worse, as an IT department 'initiative'. Either branding means person. Admittedly, the organization was a relatively small one but, although we only employed about 80 people (across three sites), we did also have an associate consultant team that was nearly a hundred strong. And, back then, we probably couldn't have done something as complex as this in a much larger organization.

The lessons that we learned in our first two implementations, and our experience with BS 7799 implementations – often in very substantial organizations - since then, in both the public and private sectors, has enabled me to crystallize the nine keys to a successful ISMS project. We've updated that knowledge and experience preparing our own business for ISO 27001 certification and, in parallel, I've also studied the emerging standard closely while writing ISO 27001: a Pocket Guide. The fact is that, properly managed and led, any ISO27001 project can be successful. We've proved it.

Over the years, my organization has developed approaches to implementing an ISMS that can help project managers identify and overcome many of the very real problems they face in achieving a successful outcome. We've also developed unique tools and techniques that simplify the process and enable organizations to succeed without us – and information security success is, in the long term, not consultant-dependent. It depends on the organization itself; this book describes the key issues, the building blocks of success, and tells you how to tackle them.

This book refers, in its course, to a number of other books or tools that I have written or that have been produced by my company. In each case where I have made a specific reference, the book or tool is unique and was developed to do the specific job that I describe it as doing. I developed these books and tools because there simply was nothing available on the market that did a comparable job of work.

This book also does not repeat the history of BS799, the story of ISO 27001, the relationship between ISO 27001 and ISO 17799, or some of the more detailed structural issues of ISO 27001, all of which can be found in ISO 27001: a Pocket Guide. Nor does this book provide the sort of detailed, control-by-control project guidance that you will get from IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799. I recommend that you read and use both these books before and during your ISMS project.

headlines it needs. Unless you have this sort of commitment, there are going to be lots of things that people throughout the organization will see as higher priorities than your project. Of course, there are going to be *some* higher priroties; what you need is clear prioritization, that is understood across the business and is continuously supported by the CEO.

The relative prioritization of your project needs to be clearly understood. Within that context, it needs to have the firm and uncompomising endorsement of the CEO. By 'endorsement' I mean that, when those (sometimes unnecessary) internal barriers appear, the words: 'this is a project endorsed by the CEO' should go a long way to overcoming them.

Change management

The third reason you need the CEO's support is that an ISMS project is a change management project. The implementation of an ISMS is not a low-impact activity. It is not something that can simply be grafted onto an existing organization or built into existing processes and procedures. It changes how computer users do almost everything and it also affects a number of aspects of managers' everyday activities. A successful ISMS project is, in other words, a low-key, but nevertheless wide ranging change management project and the way you approach it has to learn from the experience of successful change management programmes.

There have been many books written about change management programmes and initiatives. Many of these projects fail to deliver the benefits that have been used to justify the expense of commencing and seeing them through. Successful implementation of an ISMS does not require a detailed, strategic change management programme, particularly not one devised and driven by external consultants. What it does require is complete clarity amongst senior management, those charged with driving the project forward, and those whose work practices will be affected, as to why the change is necessary, what the end result must look like and why this result is essential. The change management aspects of this are the third the stated scope to ensure that all interdependencies and points of weakness have been identified and adequately dealt with.

In reality, as stated earlier, the process of designing and implementing an effective ISMS may be made simpler by including the entire organization for which the board has responsibility.

Phased approach

There is also an argument, in large, complex organizations, for a phased approach to implementation. This is a different argument from the scoping one, although there is a logical relationship between the two. Where it really is possible to adequately define a scope for a subsidiary part of the organization, such that its information security needs can be independently assessed, it may be possible to gain substantial experience in designing and implementing an ISMS, as well as a track record of success and the momentum that accompanies it, such that a subsequent roll-out to the rest of the organization can be carried through successfully and smoothly. These considerations apply to any large, complex project and the appropriate answer depends very much on individual organizational circumstances.

While there are significant benefits to this 'step-by-step' approach, they will all be lost if scoping attempts to create 'artificial' business units, ones that do not meet the criteria described above, to which the ISMS should apply. The disbenefits of such an approach are described in *Shortcuts*, below.

Network mapping

It can help (but is not essential) to make a network map that shows how your central management and information systems link together and which identifies all of the points at which the outside world can interact with your network. This map will be very simple (because the network is simple) for a small organization and far more complex for a larger, more complex organization. The initial map that you draw to aid your initial scoping exercise will need to be extended as part of the detailed project planning phase to ensure that all aspects of your information systems have been identified. You do

We recognize that, in any consideration of whether or not to bring in consultants, there is always a third consideration, which is the extent to which using consultants is part of how the organization tackles change projects. In those organizations that have a history of using – and successfully using – consultants to facilitate change, the argument in favour of using ISMS consultants is balanced more toward using them than not. However, in organizations that do not have any deep experience in managing consultants, who have traditionally tackled all change projects using their own internal resources, the argument in respect of how an ISMS project is resourced would be far more strongly against bringing in outsiders.

The reason for this is simple: consultants, like any other organizational resource, have to be managed. Previous organizational experience in successfully managing consultant engagements is essential if you are going to use consultants for anything as sensitive as a change project. Change projects require a great deal of internal communication, a great deal of internal sensitivitiy, and a great deal of leadership. No consultant is able to provide organizational leadership, although many may – in a vacuum – try. In sum, if you haven't used consultants before, don't start now. There are a number of books and tools (many available from www.itgovernance.co.uk), as well as a wealth of training, available from multiple sources, that will give you what you need in tackling this project without consultant support.

There are, nevertheless, a number of more specialist areas in which consultants can be helpful – assuming that you know how to get the best out of them.

1. You can use consultants – trusted third parties – to communicate the seriousness of the information risks faced by the organization and the need, therefore, for an ISMS – remembering that any such communication will always be more effective if it is well understood throught the organization that the consultants are not getting any further work out of frightening everyone;

Who conducts the risk assessment?

Unless the organization already has a risk management function, staffed by people with training that enables them to carry out risk assessments, it will (depending on the complexity of the organization) need to delegate the responsibility to someone. There are two ways of doing this. The first is to hire an external consultant (or firm of consultants) to do it. The second is to train someone internally. The second is preferable in most cases, as the risk assessment will need to be reviewed when circumstances change and having the expertise in-house enables this to be done cost effectively. If the organization already has a trained information security adviser, this person could take on the role.

In circumstances where the organization has existing arrangements with external suppliers for risk assessment services, or is in the process of setting up a risk management function or capability (in the context of responding to the requirements of the Turnbull Guidance, or Basel 2, perhaps), then it should from the outset ensure that its information security risk assessment process is included

Risk analysis

Qualitative risk analysis is by far the most widely used approach (and is the approach expected by ISO27001). Risk analysis is a subjective exercise in any environment where returns are derived from taking risks – and it is preferable to be 'approximately correct, rather than precisely wrong.' Risk anaysis starts with an indentification of the assets that are within the scope of the proposed ISMS, because these are the assets that are 'at risk'.

These assets will include a wide range of information and information systems, ranging from tacit knowledge through to published documents and taking into account the entire information technology infrastructure which makes it possible for the organization to process, access or otherwise use this information. An asset is something that could be described as 'something that someone else wants,' on the basis that, if no one else wants it, it can't be that valuable. Glib, perhaps; as a definition, though, it