

CHAPTER 2: MANAGEMENT SUPPORT

It may be something of a cliché but, for ISMS projects, it is certainly true to say that ‘well begun is half-way done.’ The person charged with leading an ISO 27001 ISMS project has to reduce something that looks potentially complex, time- and resource-consuming, and difficult, to something that everyone believes can be achieved in the time frame allocated and within the resources allowed. And then you have to make sure that it is actually delivered!

What this actually means is that the ISMS project leader has to set the project up in such a way that it is adequately resourced, that there is enough time (including for everything that will go wrong) and that everyone understands the risks in the project and accepts the controls that are being deployed to minimise them.

Almost everyone dislikes change. Very few people relish dealing with the unknown. Most people will see an ISMS project as something that brings both change and the unknown into their working life. On balance, they’re not going to welcome it. In any group of IT users, there are always one or two who support the idea of improving information security. The reaction of the majority will be a passive lack of real interest – their approach will be that they’re no more interested in information security than are all their mates, and if it’s not worth chatting about around the water cooler, or after work, it’s not worth getting excited about.

A handful of people will actively try to undermine the project. They will be vocal, and they’ll usually have strong views, some of which may even sound rational and sensible. In a relatively short space of time, people like these can have the effect of doubling the apparent effort required to bring the project in successfully. And, if the nay-sayers are in the IT team – particularly in the IT management team – or are influential business managers, then it’s going to be extremely difficult for the project to build up any real momentum. And without momentum, without a head of steam, you will feel like you’re starting afresh every day.

The project leader, in the first phase of the project, is the person to whom everyone else in the organization turns for insight, comfort and support. You have to be the person who provides enthusiasm, certainty and an understanding of what’s involved.

This means that learning too obviously on the job is not advisable. I don’t mean by this that you need to know all the answers at the outset, because that’s not practical. As long as you have a clear understanding of the strategic issues, practical knowledge of where to turn for advice and guidance, you can be effective even if you’re only a day or two ahead of everyone else in the detailed knowledge required for the project.

You’d be surprised at the number of times someone has kicked off an ISMS project without adequate preparation and has then failed to adequately answer a series of questions or challenges about specific issues, and then been surprised that the project has lost credibility rather quickly.

The first key to ISO 27001 success is, in other words, to *set up for success*.

Setting up for success means four things:

1. Knowing – and being able to clearly communicate - why information security is important for any organization and, in particular, for yours;
2. Knowing why ISO 27001 is the right way to provide information security– and this also means having a background knowledge of the standard and how it works;
3. Knowing how the project is going to be structured, what the key elements are (there are nine of them), and why this is the best way to go about it;
4. Knowing whether you’re going to use consultants or do it yourself, and the pros and cons of both.

While your initial study of this book will enable you to deal with points three and four, I’ll deal with the first two points here. The first was that you should know – and be able to clearly communicate, in business terms - why information security is important and, in particular, why it is important for *your* organization. Information security is, as I said in the introduction, a business issue, not a technology one. It is about securing the availability, confidentiality and integrity of your organization’s information. Information security, says the introduction to ISO/IEC 17799:2005, is ‘the protection of information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities’ and is also ‘essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image.’ It is critical that you are able to present – at all levels in the organization – these key reasons why business needs to take information security seriously.

There are two separate sets of risks that organizations have to address.

Information risk and regulatory risk

Acquiring the basic knowledge about both sets of risk is relatively easy. You can assemble it yourself from all the newspapers, journals and magazines that deal with information security. You could also read any one of a number of books on the subject. The trick, though, is to get this information into a format that will be meaningful to anyone outside the IT department, outside the risk department and outside the finance department.

The sad fact of the matter is that most business people don’t want to know about information security. Like plumbing, they just want to know that it’s there and that it’s not an issue. Of course, once you’ve made your information security project happen, it will be just like the plumbing – but you have to get them much more involved, in the first instance, than they wanted to be. I’ll return to this theme in the next chapter, but part of your initial preparation must be to assemble all the information that illustrates the need for information security into a coherent, business-relevant package.

The one book I recommend, because it has a uniquely focused business perspective on the issues, and because its content is structured around the broadly recognised information security agenda, is [*The Case for ISO 27001*](#). This book covers all the information security subject areas, from external threats (hackers, viruses, spam, etc), to the internal ones (including fraud, ex-employees), as well as cyber crime, cyber-terrorism and ‘Acts of Nature’. It describes the principal regulatory compliance risks and identifies both national and international regulation that affects organizations today.

It sets out the reasons why ISO 27001 is an appropriate way to deal with them. Reading this book is a good way to get an overall sense of, and business perspective on, how the diversity of information security risks and threats is structured and leads into the second area I identified above, which is knowing why ISO 27001 is the uniquely appropriate way to tackle your organization's information security challenges. But before you can do this, you need to translate the generic, global level risks and threats described in the *Case for ISO 27001* into organizationally relevant examples.

The purpose of an information security management system is to reduce and control risks to information security. Your organization therefore needs to understand, in as visceral a way as possible, what those risks are *in relation to its own operations*.

The 'fear list'

You need a collection of information security problems experienced in your own organization, or meaningful extrapolations of what individual security vulnerabilities in your organization might lead to, to make the more remote, large scale concerns very real for people in your own organization. I call this the 'fear list'. Its objective is to frighten people into paying attention to the need for serious action. Everything that goes on your fear list should be something that everyone can understand, should be specific to your organization, should be realistic (ie it must have happened somewhere else that you can point to) and it must have meaningfully negative consequences to your business – by which I mean significant business disruption or losses that can be approximately quantified.

For instance, data protection, as a subject, doesn't get a lot of wide-eyed attention from the average UK (or, for that matter, a US, EU, South Asian or any other) business executive. Describing a section 55 offence – even though it could apply to every director in your organization - is unlikely to improve their concentration in any way. However, identifying a company *in your industry* that failed to adequately protect individual data and which then found its name in the newspapers and its directors in court, with substantial losses of reputation and revenue, is much more likely to excite their attention.

Similarly, talking about virus or hacker risks is unlikely to raise their blood pressure if the organization has never suffered attacks from either. Talking about the way in which hackers, virus writers and spammers collaborate to randomly target every organization with the statistical result that, if you haven't been hit so far, you're likely to be next, is a better argument. It's also sensible to focus on current and high profile issues, such as spyware, wireless security and terrorism; these are currently reasonably high in the public consciousness and so more likely to make a hit with other people in the organization.

Above all, identify the two or three biggest computer outages or down periods in the last twelve months, the ones that have significantly affected the organization, and identify how, with an improved security system, these could have been avoided. Try and put hard numbers on the benefits of avoiding them, such as the total number of days of work that could have been saved, the number of items that could have been processed, and the amount of money that wouldn't have been lost, etc.

Chapters two and five will describe how to use this information pro-actively, to get buy-in to the project from where you need it – senior management, business managers, IT managers and staff and, above all, the people on whom you depend for

the ultimate success or failure of this project – the IT users across the organization. But you will need to carry around in your head, for at least the first two months of the project, the two or three biggest information security issues that you've identified so that, when someone says (as they inevitably will): 'Why are we doing this?' you have the answer immediately available.

Of course, if you can't identify any specific information security risks that your organization needs to control, there probably isn't a good reason for pursuing this project – but I doubt that's the case.

ISO 27001/ISO 17799

The information security standard is, in fact, a two-part standard which has undergone considerable evolution. One part of the standard (ISO 27001:2005, also known as BS 7799-2:2005) provides a specification for the ISMS (it uses words like 'shall', particularly in Annex A, which is the list of controls). The other, ISO 17799:2005 (also known as BS 7799-1:2005) has the status of a Code of Best Practice; the assembled guidance on best practice information security from around the world.

The difference between a specification and a code of practice, in the world of management systems standards, is that a specification contains the word 'shall' and specifies what is mandatory for a system if it is to comply with the standard, while a code of practice provides guidance and uses words like 'should' to indicate that compliance is not mandatory. Organizations can choose controls from this code of practice or from anywhere else, provided the requirements of the specification are met. Accredited certification takes place against a requirements specification, not a code of practice

ISO 27001 depends on ISO 17799 and requires organizations to refer to it for guidance on controls. It does not, however, require that guidance to be applied indiscriminately, and it also recognizes that organizations may need guidance from elsewhere to address issues the standard has failed to deal with adequately. Technically, therefore, it is not possible for any organization to seek certification against ISO 17799, although it is possible to gain a 'statement of conformity' with it.

You need to obtain, and study, copies of both [ISO/IEC 27001:2005](#) and [ISO/IEC 17799:2005](#). It is against these standards specifically that compliance will be measured and they, and their exact words, therefore have precedence over any other guidance or commentary. Copies of the standards can be obtained from your national standards body or from www.itgovernance.co.uk (IT Governance Ltd is an authorized BSI international standards distributor).

In cases of doubt or uncertainty, your certification auditor will refer to the standards for guidance and clarification; if everything you do can be tied down to specific words in the standard, you will be in a strong position. Do not, on the other hand, assume that if you do something that the standard does not specify, that that is incorrect. The standard is a *minimum* requirement, not a maximum one.

Background to the standard

BS 7799 was originally the outcome of a joint initiative by the DTI in the UK and leading UK private sector businesses. The first version of BS 7799 appeared in February 1995. It was, originally, simply a Code of Practice for IT Security Management.

BS 7799 underwent a significant review in 1998 and in 1999 a revised standard was launched. The original Code of Practice was significantly revised and retained as Part 1 of a new two-part British standard and a new Part 2, titled ‘Specification for Information Security Management Systems,’ was added, and this provided the specification against which an organization’s security management system could be assessed and certified.

As a Code of Practice, BS 7799-1 took the form of guidance and recommendations. Its foreword clearly stated that it was not to be treated as a specification. It became internationalized as ISO/IEC 17799 in December 2000. BS 7799-2, on the other hand, remained a British Standard until November 2005, when it finally became internationalized as ISO 27001.

ISO/IEC 17799

In 1998, when the original BS 7799 was revised for the first time, references to UK legislation were removed and the text was made more general. It was also made consistent with OECD guidelines on privacy, information security and cryptography. Its best practice controls were made capable of implementation in a variety of legal and cultural environments.

In 2000, BS 7799–1:1999 was submitted as the proposed text of an international standard and was re-issued with minor changes as BS ISO/IEC 17799:2000. It was issued as a single-part international standard, titled ‘Information Technology – Code of Practice for Information Security Management’. BS 7799–2:1999 was then replaced by the 2002 version and this, with the revised Annex A, is the standard against which an ISMS has been certified for the last three years.

In other words, the ISO/IEC 17799 Code of Practice is intended to provide a framework for international best practice in Information Security Management and systems interoperability. It also provides guidance, to which an external auditor will look, on how to implement a certifiable ISMS. It does NOT, as described above, provide the basis for an international certification scheme.

Links to other standards and toolkits

ISO 27001 is designed to harmonize with ISO 9001:2000 and ISO 14001:1996 so that management systems can be effectively integrated. It implements the Plan-Do-Check-Act (PDCA) model and reflects the principles of the 2002 OECD guidance on the security of information systems and networks.

ISO 27001 implicitly recognizes that information security and any Information Management Security System (ISMS) should form an integrated part of any internal control system created as part of Corporate Governance procedures. The standard fits in with the approach adopted by the Turnbull Committee.

There is further discussion on the relationships with these other standards, more detail on the interrelationship with ISO 17799, and initial guidance on how frameworks such as ITIL (and ISO 20000) and CobiT could be used in an ISO 27001 implementation in [ISO 27001: a Pocket Guide](#). In addition, BSI has just published a new risk management standard, [BS7799-3:2006](#).

Finally, you should ensure that you look at appropriate [risk assessment tools](#) and [documentation toolkits](#) as part of your initial *setting up for success*.