# Nine Steps to Success

## An ISO27001:2013 Implementation Overview

Alan Calder

Second edition

itgp™

# Nine Steps to Success

## An ISO27001:2013 Implementation Overview

Second edition

# Nine Steps to Success

An ISO27001:2013
Implementation Overview

Second edition

**ALAN CALDER**

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernance.co.uk



First published in the United Kingdom in 2005
by IT Governance Publishing.

Second edition published in 2013.

ISBN 978-1-84928-511-7

## ABOUT THE AUTHOR

Alan Calder is the founder and Executive Chairman of IT Governance Ltd (*www.itgovernance.co.uk*), an information, advice and consultancy company that helps company boards tackle IT governance, risk management, compliance and information security issues. He has many years of senior management experience in the private and public sectors.

IT Governance Ltd operates websites around the world that distribute a range of books, tools and other publications on IT governance, risk management, compliance and information security.

## CONTENTS

# INTRODUCTION

The International Standard ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements has now replaced the earlier 2005 version. Information security has always been an international issue, and this new version of the Standard reflects eight years of improvements in the understanding of effective information security management. It also takes account of the evolution in the cyber threat landscape over that period, and allows for a new range of best practice controls.

Information security is also a management issue, a governance responsibility. The design and implementation of an Information Security Management System ('ISMS') is a management role, not a technological one. It requires the full range of managerial skills and attributes, from project management and prioritisation, through communication, sales skills and motivation, to delegation, monitoring and discipline. A good manager who has no technological background or insight can lead a successful ISMS implementation, but without management skills, the most technologically sophisticated information security expert will fail at the task.

This is particularly so if the organisation wants to derive maximum, long-term business value from the implementation of an ISMS. Achieving external certification is an increasingly necessary cost of doing business. Achieving the level of information security awareness and good internal practice that enables an organisation to safely surf the stormy, cruel seas of the

information age, requires a level of culture change no less profound than that required to shift from industrial to post-industrial operations.

I know all this because my background is as a general manager, not as a technologist. I came to information security in 1995 because I was concerned about the information security exposures faced by a 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 CEOs in my position, it is really aimed at the manager – often an IT or information security manager – who is charged with tackling an ISO27001 implementation, and who wants a sure route to a positive outcome. It identifies what the experience of many ISO27001 implementations has taught me are the nine key steps to ISMS success. The lessons seem to apply in any organisation, public sector or private, and anywhere in the world. They start with recognising the challenges usually faced by anyone concerned to improve their organisation'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 organisation'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 organisational pounds 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 than the security flavour of the month – for instance, penetration testing sales increased when hacktivist successes hit the headlines. Once deployed, any single solution is unlikely to alter the overall security posture of an organisation by more than one degree, not least because any effective security solution requires an integrated combination of technology, procedure and user application. Integration of this order also 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 the ISMS will be still born. Almost everyone who works in any business believes that management fads just have to be endured until they go away, and that IT department initiatives just create more problems and barriers for people trying to do their everyday work. Scott Adams, the creator of Dilbert, does say after all that most of the ideas for his sketches are sent to him by people who are simply describing their daily working lives.

An ISMS project does slightly better if it is seen as having a credible business need: to win an outsourcing contract, for instance, or to comply with a public funding requirement. In fact, such short-term justifications for introducing an ISMS, for seeking external certification, infrequently bring the company any real long-term benefit, because the project rarely develops the sort of sustained momentum that will

drive user awareness and good practice into all the reaches of the organisation.

When we first decided to tackle information security, way back in 1995, my organisation was required – as a condition of its branding and trading licence – to achieve both ISO9001 certification and Investors in People (IiP) recognition. We intended to sell information security and environmental management services as well and, out of a desire to practice what we preached, as well as from a determination to achieve the identifiable business benefits of tackling all these components of our business, we decided to pursue both BS7799 and ISO14001 at the same time.

BS7799 existed then in only an unaccredited form and it was, essentially, a Code of Practice. There was only one part to it and, while certification was technically not possible, a statement of conformity was. The other standards that we were interested in did all exist but, at that time, it was generally expected that an organisation would approach each standard on its own, developing standalone manuals and processes. This was hardly surprising, as it was unusual for any organisation to pursue more than one standard at any time!

We made the momentous decision to approach the issue from primarily a business perspective, rather than a quality one. We decided that we wanted to create a single, integrated management system that would work for our business, and that was capable of achieving multiple certifications. While this seemed to go in the face of much of that time's actual practice around management system implementation, it seemed to be completely in line with the spirit of the Standards themselves.

We also decided that we wanted everyone in the organisation to take part in the process of creating, and developing, the integrated management system that we envisioned, because we believed that was the fastest and most certain way of getting them to become real contributors to the project, both in the short and the long term. We used external consultants for part of the ISO9001 project but there simply was no BS7799 expertise available externally.

This lack of BS7799 experts was a minor challenge in comparison to the lack of useful books, or tools, that we could use. While you can today purchase books, such as *ISO27001/ISO27002: A Pocket Guide*, back then there were only bookshelves full of thick, technologically-focused books on all sorts of information security issues, but nothing that might tell a business manager how to systematically implement an Information Security Management System. We had no option but to try and work it out for ourselves.

We actually did the job twice, once under the unaccredited scheme, and the second time after the Standard had become a two parter (the earlier, single part had become a Code of Practice and a new part, a specification for an Information Security Management System, had been introduced) and been accredited. In fact, our accredited audit was also our certification body's first observed audit for their own UKAS accreditation. While that was an interesting experience, it did mean that our systems had to be particularly robust if they were to stand the simultaneous scrutiny of two levels of external auditors!

We underwent external examination on five separate occasions within a few months, and our integrated

management system achieved all the required external certifications and recognitions. We did this without anything more than the part-time assistance of one ISO9001 consultant and an internal quality management team of one person. Admittedly, the organisation 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 100 strong. Back then, we probably couldn't have done something as complex as this in a much larger organisation.

The lessons that we learned in our first two implementations, and our experience with ISO27001 implementations – often in very substantial organisations – since then, in both the public and private sectors, has enabled me to crystallise the nine key steps to a successful ISMS project. We updated that knowledge and experience preparing IT Governance itself for ISO27001 certification and, in parallel, I've also studied the latest version of the Standard closely while writing *ISO27001/ISO27002: 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 organisation 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 organisations to succeed without us – and information security success is, in the long term, not consultant-dependent. It depends on the organisation 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 IT Governance Ltd. 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 does not repeat the history of the development of the Standard, describe the relationship between ISO27001 and ISO27002, or discuss some of the more detailed structural issues of ISO27001, all of which can be found in *ISO27001/ISO27002: A Pocket Guide*. Nor does this book provide the sort of detailed, control-by-control project guidance that you will get from *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. I recommend that you read, and use, both these books before and during your ISMS project.

# CHAPTER 1: INITIAL APPROACH

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/IEC 27001:2013 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 with the resources allowed. 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 are 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 are no more interested in information security than are all their friends, and if it is not worth chatting about around the water cooler, or after work, it is not worth getting excited about.

A handful of people will actively try to undermine the project. They will be vocal, and they will usually have strong views, some of which may even sound rational and

sensible. In a relatively short space of time, people like these can double the effort required to bring the project in successfully. If the nay-sayers are in the IT team – particularly in the IT management team – or are influential business managers, then it is going to be extremely difficult for the project to build up any real momentum. Without momentum, without a head of steam, you will feel like you are starting afresh every day.

The project leader, in the first phase of the project, is the person to whom everyone else in the organisation turns for insight, comfort and support. You have to be the person who provides enthusiasm, certainty and an understanding of what is 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 is not practical. As long as you have a clear understanding of the strategic issues, and practical knowledge of where to turn for advice and guidance, you can be effective, even if you are only a day or two ahead of everyone else in the detailed knowledge required for the project.

You would 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 ISO27001 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 organisation and, in particular, for yours.
2 Knowing why ISO27001 is the right way to provide information security – and this also means having 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 are 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 organisation. 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 organisation's information. The best description of information security, though, still comes from the earlier version of the Standard, which says that it is 'the protection of information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise 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 organisation – these key reasons why business needs to take information security seriously.

There are two separate sets of risks that organisations 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 is there and that it is not an issue. Of course, once they'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 ISO27001:2013*. This book covers all the information security subject areas, from external threats (hackers, viruses, spam, etc.), the internal ones (including fraud, ex-employees), cyber crime, cyber terrorism and 'Acts of Nature'. It describes the principal regulatory compliance

risks and identifies both national and international regulation that affects organisations today.

It sets out the reasons why ISO27001 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 ISO27001 is the uniquely appropriate way to tackle your organisation'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 ISO27001:2013* into organisationally relevant examples.

The purpose of an Information Security Management System is to reduce and control risks to information security. Your organisation 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 organisation, or meaningful extrapolations of what individual security vulnerabilities in your organisation might lead to, to make the more remote, large-scale concerns, very real for people in your own organisation. 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 organisation, should be realistic (i.e. 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 business executive. Describing a section 55 offence – even though it could apply to every director in your organisation – 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 was the subject of an ICO (Information Commissioner's Office) enforcement order or fine, 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 organisation has never suffered attacks from either. Talking about the way in which hackers, virus writers and spammers collaborate to randomly target every organisation with the statistical result that, if you haven't been hit so far, you are likely to be next, is a better argument. It is also sensible to focus on current and high-profile issues, such as cyber risk, wireless security and cyber terrorism; these are currently reasonably high in the public consciousness, and so are more likely to make a hit with other people in the organisation.

Above all, identify the two or three biggest computer outages or down periods in the last 12 months, the ones that have significantly affected the organisation, 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, etc.

Chapters two and five will describe how to use this information proactively, 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 organisation. 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 have 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 organisation needs to control, there probably isn't a good reason for pursuing this project – but I doubt that is the case.

## ISO27001/ISO27002

The information security Standard is, in fact, a two-part Standard which has undergone considerable evolution. One part of the Standard (ISO27001:2013) provides a specification for the ISMS (it uses words like 'shall', particularly in Annex A, which is the list of controls). The other, ISO27002:2013 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. Organisations can choose controls from this

Code of Practice or anywhere else, provided the requirements of the specification are met. Accredited certification takes place against a requirements specification, not a Code of Practice.

ISO27001 depends on ISO27002, and requires organisations to refer to it for guidance on controls. It does not, however, require that guidance to be applied indiscriminately, and it also recognises that organisations may need guidance from elsewhere to address issues the Standard has failed to deal with adequately. Technically, therefore, it is not possible for any organisation to seek certification against ISO27002, although it is possible to gain a 'statement of conformity' with it.

You need to obtain, and study, copies of both ISO/IEC 27001:2013 and ISO/IEC 27002:2013. 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 authorised standards distributor for a number of standards bodies).

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.

**Skills, knowledge and competence**

Effective implementation of an ISMS is accelerated if you – as well as your project team and others who will have key roles within the ISMS – all acquire the specialist knowledge about information security management that will enable you to drive this project forward. It is, in any case, a basic requirement of the Standard that an implementing organisation delegates tasks and responsibilities to those with identified roles within the ISMS.

The most useful training courses are those which provide an introduction to the whole subject, those which cover implementation, and those which cover audit. All good courses are accredited by an external examination board, such as IBITGQ (the International Board for IT Governance Qualifications – *www.ibitgq.org/*).

An ISO27001 ISMS Foundation course is a one-day course that provides a broad awareness of the subject and is suitable for all project team members.

An ISO27001 Lead Implementer course is the ideal course for those who will be responsible for taking the project forward. This is a three-day course that provides practical guidance on effective implementation.

All management systems have to be subject to internal (management) audit and an ISO27001 Lead Auditor course will provide those who, inside your organisation, will be charged with designing and managing your internal information security audit process, with the skills they need to do this effectively.

You can see more detailed information about these, and other courses, here: *www.itgovernance.co.uk/training.aspx*.

**Links to other standards**

ISO27001 is supported by a family of related best practice standards, each of which provides additional guidance on a specific aspect of information security management. This family of standards is continuously growing and developing, and up-to-date information is available from *www.itgovernance.co.uk/iso27000-family.aspx*.

ISO27001:2013 specifically relies on the various definitions that are contained within ISO27000, and so it may also be useful to acquire a copy of ISO27000:2012.

ISO27001 is designed to harmonise with ISO9001:2000 and ISO14001:1996, so that management systems can be effectively integrated.

ISO27001 implicitly recognises that information security, and any Information Security Management 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 in the UK by the Turnbull Guidance.

There is further discussion on the relationships with these other standards and more detail on the interrelationship with ISO27002 in *ISO27001/ISO27002: A Pocket Guide*.

# CHAPTER 2: MANAGEMENT SUPPORT

Information security is both a management and a governance issue. Successful implementation of an ISMS depends absolutely on the project having real support from the top of the organisation. With it, you have a real chance of success; without it, none at all. Securing real top management support – not mere lip service – is the second key to ISO27001 success. In this context, I'm not necessarily talking about the CEO of a large, multi-subsidiary organisation; I'm talking about the person who is accountable for the business success, or failure, of the trading entity (*see Chapter Three*, which deals with scope) that is considering ISO27001. This could be a trading division, a subsidiary company, a standalone unit, or a virtual organisation.

It is important to be clear about the meaning, in this context, of 'accountable'. I mean the person whose job and career ultimately depends on the success of the business entity that is considering ISO27001; this person does not always occupy the role that is formally 'where the buck stops'. All organisations know exactly where the buck really stops, and this is the person I'm referring to as the CEO in this chapter.

## Strategic alignment

The first reason why the CEO has to fully support you, and the ISMS project, is that it is a business project, not an IT project. It has to be fully aligned with the business model, business strategy and goals, and has to be prioritised for the business, and allocated an appropriate level of resources.

The only person who can effectively do this is the CEO. No single project leader is in a position to be clear about the organisation's strategic needs and goals but, as this is a strategic project that affects everyone, you need to be 'in the loop' so that you can tailor your own plans to deliver the organisation's business priorities.

You also need to know what the strategic risks faced by the organisation are, and how these are reflected and prioritised in information security risks. There are many possible questions whose answers will be critical to your approach and detailed plan. For instance, is the risk of intellectual property theft more significant (with a greater potential impact) than the risk of (for example) a three-day business closure? Is regulatory compliance more, or less, important than reducing the cost of sales? Is information security and regulatory compliance going to be important in outsourcing solutions (or, when faced with a choice between a lower cost but less secure, and a more secure but more expensive outsourcing option, which one will the organisation choose?)? How should conflict between the regulatory requirements of two different jurisdictions in which the organisation trades be resolved? What is the trade-off between the operational flexibility that is allowed to subsidiary organisations, and implementation of a minimum, consistent level of information security and IT service reliability? What are the long-term plans for specific support services? (If they are going to be outsourced, then you are going to approach ISMS implementation differently than if they are staying in-house.) There are many such questions whose answers you need to know before you can even start planning; there are many others that will come up in the course of the project.

## Prioritisation and endorsement

The second reason you require this level of support is that, without it, the project simply won't happen. It is not enough for the CEO and executive management simply to acknowledge that the project is important. It is not enough that they merely talk about it. It is not enough that you know enough to be able to align the project with the business plan. They have to be committed, well and truly determined to achieve it, if it is really to happen. Top management commitment means that the project gets the resources (financial and human) it needs. It gets the oversight, 'face time', and internal communication headlines it needs. Unless you have this sort of commitment, there are going to be lots of things that people, throughout the organisation, will see as higher priorities than your project. Of course, there are going to be some higher priorities; what you need is clear prioritisation, which is understood across the business, and which is continuously supported by the CEO.

The relative prioritisation of your project needs to be clearly understood. Within that context, it needs to have the firm and uncompromising 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

organisation, 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 reason why the CEO's support and backing is essential: you want him to be setting the example, doing all the things that you are going to want everyone else to be doing.

The fact is that the Standard itself demands this level of support. It will not allow any certification body to certify an ISMS without getting firm evidence of the commitment of senior management. The reason for this is simple: the ISMS will not be adequate, the risks to the organisation will not have been properly recognised or fully addressed, and the strategic business goals, and the consequent future information security requirements, are unlikely to have been considered.

## The CEO's role

Ideally, the CEO should be the driving force behind the programme and achievement of ISO27001 certification should be a clearly stated goal of the current business plan. The CEO needs to completely understand the strategic issues around IT governance and information security, and the value to the company of successful certification. The CEO has to be able to articulate them – to the Board and to senior management – and to deal with objections and issues arising. Above all, he or she has to be sufficiently in command of this part of the business plan to be able to keep it on track against its strategic goals.

The chairman and board should give as much attention to monitoring progress against the ISO27001 implementation plan as they do to monitoring all the other key business goals. Clause 5.1 of the Standard specifically requires evidence of this commitment from the top: 'Top management shall demonstrate leadership and commitment with respect to the Information Security Management System'. If the CEO, chairman and board are not behind this project, there is little point in proceeding; certification will not happen without clear evidence of such a commitment. This principle, of leadership from the top, is of course also essential to all major change projects.

If you are already the CEO of the organisation, then you are doing exactly the right thing by reading this book and preparing to drive the information security project yourself. If you are not the CEO, then you have got to secure the sort of commitment and support that I described on the previous page.

There are organisations in which the CIO is a member of the senior management team, is responsible for an

integrated function that includes information security, and already has the full trust and support of the CEO and the Board. In such an organisation, the CIO can be the driver of the project, but it will still need the CEO's commitment and support, not least so that everyone in the organisation recognises that securing recognition is a business priority. The CIO will also urgently need to build a cross-business project team, but I will return to this in *Chapter Five*.

***The CEO's commitment***

The starting point is simple: you need to talk to the CEO. You should refuse (however nicely you do it) to get started on the project until you have had a proper meeting with the CEO. I mean it: don't do anything. Don't even talk about the project to anyone else. If necessary, be vague; say things like: 'that's really interesting but, as I'm sure you know, an initiative like that has to come from the top, so when can we meet with the CEO?' The potential political repercussions of this pre-project phase are such that managers tasked with achieving ISO27001 have brought in external consultants specifically to get this message across. External consultants do, after all, specialise in telling organisations what they already know!

*Chapter Four* will deal with the options around the use, or otherwise, of consultants. At this point, if you are considering using consultants, with the specific objective of getting a message across to the CEO, it is essential that you retain a company who understand their role in the exercise. You give them a very specific project brief, which is to identify the key requirements and provide a top level route map, for a successful ISMS implementation in your organisation.

You should be crystal clear with them about the need for their presentation to focus on the role of the CEO and the top management. You should ensure that their presentation will be to that team. Of course, they are also likely to want to put themselves forward for the task, but you should be able to set out clearly the cost and business benefits of doing the job internally and you should also be able to use these advantages to swing management's support strongly behind you.

Whether the message comes from you directly, or via external consultants, you need to explain that active and committed support is essential to the project, you need to explain why (the three reasons above), and you need to map out what it entails. Unless the CEO is personally leading the project, you should, as a minimum, ask for the following active support:

- That the CEO personally applies himself to understanding the business benefits of pursuing an information security strategy, and the return on investment (more on this below) that this project will achieve for the organisation.
- That the CEO leads a presentation (which you will prepare) on the information security strategy to the Board, includes ISMS certification in the organisation's business goals for the year, secures board support for the objective (expressed in a board-approved project plan, created as described in *Chapter Three*) and arranges for ongoing board monitoring of project progress (which will ensure the project achieves, and maintains, the sort of political profile that will improve its chances of success) throughout its life.

- That the CEO personally leads presentations (which you will prepare) on the project to the executive or senior management of the organisation, as well as to all the staff in each of the organisational forums that are used for staff communication.
- That the CEO nominates his/her most senior business line executive to support the project and lead the steering group (on which, more below), to provide day-to-day backing and support for you, and to lead the change management effort – and this person has to be personally committed to the success of the project, prepared to do whatever is necessary to succeed.
- That the CEO clearly sets out – for senior management and for everyone in the organisation – the prioritisation for this project, and your authority to seek the input and involvement of all whose contribution will be essential to your success.
- That the CEO sets a personal example of applying all the work practices and following all the procedures that will become part of the new ISMS.

**Senior management support**

Senior management support is equally important. An ISMS project cuts across all parts of the organisation and, therefore, you need to be sure that all its key leaders are onside. Of course, there will always be varying degrees of enthusiasm for an ISMS project, and not all senior management will be as enthusiastic as you would like them to be. There are two important steps in securing the support that you will need from this group.

1 Set up a cross-organisational steering group to drive the project forward. This steering group should be led

either by the CEO, or by the CEO's nominated deputy, and should be primarily a business-orientated group. In other words, it should consist primarily of business managers who have a direct personal interest in the effectiveness of any ISMS project, and whose contribution will ensure that the ISMS meets the business needs, and becomes a fully functional part of the organisation. This group should include any individuals who are likely to resist the project and, if possible, they should be given key responsibilities leading to success of the project. If this is unlikely to work, alternative methods of isolating them should be pursued – this is one area in which a committed CEO should be asked to provide personal input. Finally, I can't stress enough the importance for this group, of it not having a preponderance of IT or technical people – the project must be seen as a business project, not an IT one. This group might, depending on the size of the organisation, also be the project group – whose functions are described in *Chapter Four.* In larger organisations, the steering group will be responsible for 'operationalising' the Board approved plan for implementation of an ISMS, delegating detailed work to a project group and monitoring progress on a regular basis. Those who are members of the steering group should be barred from sending junior members of their teams in their place.

2 The CEO should make the initial presentation to the steering group, and this presentation should focus on the information security risks faced by the organisation, on the potential impacts on the organisation of a failure to implement proper security, and should set out the relative prioritisation and

importance that the project has. It should be clear to everyone in the steering group that this project carries the CEO's personal endorsement, and that it will receive high-level oversight throughout its life.

# CHAPTER 3: SCOPING

Scoping is one of the nine keys to project success. It is key, both because you need to know the boundaries of what you are planning to implement, and because the Standard itself requires it.

Clause 5.2 of ISO27001 clearly sets out the requirements in respect of the ISMS policy. The policy must be approved by the Board. The policy must provide an overall sense of information security direction for the organisation, as well as including information security objectives. It must include meeting information security requirements (which might be business, contractual or regulatory in nature), and it must also contain a commitment to continually improve the ISMS.

The ISMS policy applies across the organisation that is within the scope of the ISMS. The scope (see 4.3) must take into account the characteristics of the business, its organisation, location, assets and technology – what the Standard calls the 'external and internal context' of the organisation. ISO27001 refers, at this point, to ISO31000, the international best practice Standard for organisational risk management and, for those organisations seeking to properly integrate risk management across all aspects of the business, this ISO31000 link will be important.

Your policy requirements should drive your approach to scoping the ISMS and the project. Scope determination is harder for larger, complex organisations, than it is for smaller ones. Scoping is, though, essential for any size of organisation: you have to decide which information assets

you are going to protect – and which ones you are not – before you can decide on appropriate protection.

This should be a quick decision for a small or medium sized business: the whole organisation. That is because there will probably be hard-wired connections between all the information systems, and day-to-day working relationships within the business that make it either extremely difficult, or impractical, to try and segregate one part of the business from another. The notion of segregation is at the heart of effective scoping: ultimately, you are going to try and create an impregnable barrier around that part of your business that is within the scope of your project and everything else. You have to be categorical about what is inside your information fortress and what is outside, and this means that you don't want any information systems, devices, or business units that are both inside and outside – because that will be your weakest link.

ISO27001 explicitly requires you to consider 'interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations'; in other words, you must identify what is outside the scope of your ISMS, and be prepared to justify its exclusion. This is to help you ensure that you don't try and draw the boundaries too narrowly.

**Endpoint security**

In today's business environment, your defensive barrier has to operate at the individual device level, and is highly dependent on user compliance with business procedures. In other words, your scoping decision needs to include all the information devices that people use in their jobs, such as smartphones, wireless laptops, home offices, etc. – as well

as the more obvious central office systems – accounting, payment processing, production, sales and order management, e-mail, office automation, etc.

In larger, more complex businesses, you will also want to ensure that the entity that is within scope has a clearly defined legal and management structure, and that there is alignment with the compliance requirements – part of the reason for your information security system is to ensure that you are compliant with the myriad of laws and regulations, so it makes sense for that entity which has those compliance obligations, to be fully within the scope of your information security project.

In other words, those parts of the organisation to which your ISMS is going to apply, need to be clearly identified. You should bear in mind that an ISMS is a management system, a formal structure that management deploys to ensure that its policy in information security is applied consistently throughout an organisation for which that management is accountable. Scoping of the ISMS may therefore be done on the basis of corporate, divisional or management structure, or on the basis of geographic location.

A virtual organisation, or a dispersed, multi-site operation, may have different security issues than one located on a single site. In practical terms, a security policy and ISMS that encompasses all of the activities within a specific entity for which a specific board of directors or management team is responsible, is more easily implemented than one that is to be applied to only part of the entity.

It is important to ensure that the Board of Directors that is implementing the policy does actually have adequate control over the organisation specified within the scope of

the information security policy that it will be expected to approve, and that it will be able to give a clear mandate to its management team to implement it within that entity. In other words, it is essential to decide the boundary within which protection is to be provided.

### *Defining boundaries*

The business environment and Internet are each so huge and diverse that it is necessary to draw a boundary between what is within the organisation and what is without. In simple terms, boundaries are physically or logically identifiable. Boundaries have to be identified in terms of the organisation, or part of the organisation that is to be protected, which networks and which data, and at which geographic locations.

The organisation that is within the scope must be capable of physical and/or logical separation from third parties and from other organisations within a larger group. While this does not exclude third party contractors, it does make it practically very difficult (although not necessarily impossible) to put an ISMS in place within an undifferentiated organisation that shares significant network and/or information assets or geographic locations. A division of a larger organisation that, for instance, shares a group head office and head office functions with other divisions, could not practically implement a meaningful ISMS. Usually, the smallest organisational entity that is capable of implementing an ISMS is one that is self-contained. It will have its own board of directors or management team, its own functional support, its own premises and its own IT network, or will have IT services supplied to it by a group or other supplier, subject to some form of service level agreement.

It is increasingly normal for divisions of larger organisations to independently pursue certification; the critical factor is the extent to which they can practically differentiate themselves, and their business and information systems, from other divisions of the same parent organisation.

For larger – usually highly decentralised – organisations, that have a multiplicity of systems and cultures and an extensive geographic spread, it is, as a general rule, often simpler to tackle ISO27001 and, in particular, risk assessment, on the basis of smaller business units that meet the general description set out above. Larger – more centralised – organisations that have a single business culture and largely common business and information systems throughout, are probably better off creating a single ISMS.

It is critical that, if there are aspects of the organisation's activities or systems that are to be excluded from the requirements of the security policy, that these are clearly identified – and explained – at the scoping stage. Multi-site or virtual organisations will need to carefully consider the different security requirements of their different sites and the management implications of them. There should be clear boundaries ('defined in terms of the characteristics of the organisation, its location, assets and technology') within which the security policy and ISMS will apply. Any exclusions should be openly debated by the Board and the steering group, and the minutes should set out how, and why, the final scoping decision was taken.

It is possible that, in fact, divisions of the organisation, components of the information system, or specific assets, will not be able to be excluded from the scope, either

because they are already so integral to it, or because their exclusion might have the effect of undermining the information security objectives themselves. It must, therefore, be clear that any exclusions do not in any way undermine the security of the organisation that is implementing the ISMS.

For an ISMS certification, auditors can be expected to assess how management applies its information security policy across the whole of the organisation that is defined as being within the scope of the policy, and should be expected to test, to their limits, the boundaries of 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 organisation for which the Board has responsibility.

### *Phased approach*

There is also an argument in large, complex organisations, 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 organisation, 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 organisation can be carried through successfully and smoothly. These considerations apply to any large, complex project, and the appropriate answer

depends very much on individual organisational 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 *Cutting corners*.

**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 organisation, and far more complex for a larger, more complex organisation. 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 not need a detailed initial map; you just need to know how you will get from the initial one to the detailed one.

There is a range of network mapping software that will automatically map your network for you, some of which have additional, helpful management features. The benefit of using such a tool is that it will quickly, completely and competently identify for you how your network is structured, what types of services are running and what access points and devices there actually are – and a status report of what is actually happening is much more useful than relying on a theoretical map.

Network maps are often drawn using software tools such as SmartDraw and Microsoft® Visio®, although one can start with a whiteboard and hand-draw a network diagram before attempting to model it with a software tool. Your network map will ultimately need to identify, in detail, all the devices (e.g. workstations 43, servers 6) that are connected to it, as well as their functions (e.g. print and file server, domain controller, etc.), their model and manufacturer details (e.g. Toshiba Portege, Dell Poweredge), key specifications (RAM, processor speed, etc.), their operating systems (e.g. Windows XP), the applications they run (e.g. Office 2010, Server 2013, Anti-virus 2013) and the nature of the physical connections between them (e.g. Ethernet, Cat 5 cable, wireless, T1 line). Remember that your map should include all devices that are fixed to computers (e.g. hubs, routers, switches, back-up units, RAID controllers, etc.) and should, if possible, include the manufacturer's serial numbers of the devices. More complex organisational maps are likely to identify the multiple protocols used by the organisation.

The network map should also, eventually, integrate with the technology asset list (which will form the basis of the risk assessment – as discussed in *Chapter Six*) and should be a live document, which is updated as and when the network is changed. It is also one of your most sensitive documents, so it should be under document control with a high-security classification.

**Cutting corners**

All our experience teaches that it is a mistake to define the scope too narrowly. By 'too narrowly', I mean a scope that (for instance) includes only a head office, or only that bit of the organisation that is under pressure from third party

(usually government) funders, or customers, to become certified. While it may appear, on the surface, that this is a route to a quick and easy certification, it is often, in fact, a route to a worthless certificate. That is why there is a requirement to justify exclusions from the scope.

In the long run, any external party assessing the nature of an organisation's ISMS, will want to be sure that all the critical functions that may affect its relationship are included and a limited scope will not do this. We are aware that some certification organisations are prepared to consider scopes that cover less than a complete business unit and, in our opinion, they are doing a disservice to their clients, as well as to the integrity of the ISO27001 schemes. Do not be tempted to use such certification bodies.

In conclusion, I recognise that scoping the ISMS can, in large, complex organisations, be very difficult. It is certainly an area where experienced, professional support can be helpful in assessing the best way forward, although I would recommend only using consultants who adopt much of the approach set out in this chapter. This is important because the wrong scoping decision can, in the long run, invalidate the certificate you do achieve, leave key parts of your organisation open to all the risks that you are attempting to exclude and, when you finally focus on the need to do the job properly, will be far more expensive than if you'd done it right in the first place. Worse, because you did it wrong in the first place, it will be far harder to get adequate commitment and support for an extended project across the organisation than it would have been if you had sold the whole project to the organisation in the first place.

# CHAPTER 4: PLANNING

Planning has, for a long time, been seen as an essential pre-cursor to project success. Of course, while it is necessary, it is not sufficient – a well-planned project can still fail for any one of a number of reasons. At the highest level, ISMS project planning means dealing successfully with all the issues identified in this book; each of the nine keys is also a critical component of a successful ISMS project plan. At a more practical level, planning is, in its own right, one of the nine keys to ISO27001 success. For the purposes of an ISMS implementation, 'planning' includes dealing with issues like the deployment of consultants, how the project will be managed, how different management systems will be integrated, and the identification of key responsibilities and resource requirements throughout the project lifecycle.

Anyone tackling an ISO27001 project should, once the organisation has decided to go ahead, obtain, and read *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. The book is unique, and provides comprehensive and detailed advice on most of the issues that you will encounter in implementing an ISMS. The advice in *Nine Steps to Success* is consistent with, and dovetails very directly into, the contents of the *International Guide*. It can be obtained from www.itgovernance.co.uk or from any reputable bookshop.

Helpfully, ISO27001 promotes the adoption of a 'process approach' for the design and deployment of an ISMS. While ISO27001:2013 is open to the deployment of any continual improvement approach, one of the most widely

known (and most often used in the management system world) is the 'Plan-Do-Check-Act' (PDCA) model, which will be familiar to quality and business managers everywhere. Whichever continual improvement model is selected, it should be thoroughly understood before work starts and should inform every step.

Equally helpful, ISO27001 is designed for better alignment, or integration, with related management systems (e.g. ISO9000 and ISO14001) within the organisation.

It should also be noted that, unlike the earlier version, ISO27001:2013 allows an implementation project to address the requirements of the Standard in any order – it specifically says that the sequence of the clauses should not be taken as setting out implementation precedence. However, starting at the beginning is still a very practical approach!

### Structured approach to implementation

If you were to apply the PDCA model, a structured approach to ISMS implementation would be as follows:

#### *Plan*

1 Get senior management support.
2 Define the scope of the ISMS.
3 Define the information security policy.
4 Define a systematic approach to risk assessment.
5 Carry out a risk assessment to identify and evaluate information security risks.
6 Identify and evaluate options for the treatment of these risks.
7 Select, for each risk, the controls to be implemented.
8 Prepare a statement of applicability (SoA).

9 Formulate a risk treatment plan for approval by risk owners.

***Do***

1 Implementation of the risk treatment plan and planned controls.
2 Appropriate training for affected staff, as well as staff awareness programmes.
3 Managing operations and resources in line with the ISMS.
4 Implementation of procedures that enable prompt detection of, and response to, security incidents.

***Check***

The 'check' stage has, essentially, only one step (or, set of steps): monitoring, reviewing, testing and audit. However, monitoring, reviewing, testing and audit is an ongoing process that has to cover the whole system, and a certification body will want to see evidence of at least one cycle of tests and audits on the ISMS having been completed, prior to a certification visit.

***Act***

Testing and audit outcomes should be reviewed by management, as should the ISMS, in the light of the changing risk environment, technology or other circumstances; improvements to the ISMS should be identified, documented and implemented. Thereafter, it will be subject to ongoing review, further testing and improvement implementation, a process known as 'continuous improvement'.

**Integration with existing security management systems**

ISO27001:2013 does not require a sequential approach to the establishment and implementation of an ISMS. In reality, once they realise the scale of the information risks they face, many organisations will want to tackle a number of the necessary tasks in parallel. Certainly, most organisations will come to ISO27001 with some information security structures and controls already in place, and with a question as to how to intelligently integrate these with any new ones.

While certification bodies previously assessed the ISMS on the basis that its establishment has followed the Standard sequentially, they will no longer make that assumption,

Therefore, if component tasks of establishing the ISMS are being carried out in parallel, or the organisation already has elements of an ISMS in place, it will be critically important that the risk assessment is completely objective, thorough, and that its findings are allowed to override any controls that have been implemented beforehand.

The reality is that most organisations that embark on ISO27001 already have a number of information security measures in place; ISO27001 necessitates ensuring that those controls that are in place are adequate and appropriate, and that additional required controls are implemented as quickly as possible. In other words, an analysis of the gap (popularly known as a ‘gap analysis’) between what is in place and what will be required must be carried out.

### *Gap analysis*

This gap analysis can be conducted either bottom-up or top-down and should look at the management system itself, as well as the implemented controls. A bottom-up analysis will start by gathering information on the management system and all the controls currently in place inside the organisation, and then assess whether or not they are adequate against the requirements of the organisation's statement of applicability and the Standard. A top-down approach starts with the management system requirements and the controls identified in the statement of applicability, and assesses the extent to which they have already been implemented. Our preferred approach is the top-down one, as this will most quickly identify the critical loopholes in the existing security systems, as well as the controls that have been deployed, but are unnecessary, and can therefore be eliminated or limited.

The statement of applicability will only be complete once all the identified risks have been assessed and the applicability of all the identified controls has been considered and documented. Usually, the statement is started before any controls are implemented, and completed as the final control is put in place.

### Quality system integration

Many organisations that tackle ISO27001 already have an ISO9000 certificated quality assurance system in place. ISO27001 was designed to encourage integration of quality and other management systems. The ISMS should be integrated with the quality assurance system to the greatest extent possible. In particular, ISO27001, clause 7.5, which deals with documentation and document control records,

can (and should) be met, by applying any existing documentation control requirements of an existing ISO9000 management system. Procedures within the ISMS have to be numbered, and documents have to be controlled. The logical approach is that the ISO9000 approach will be adopted by any organisation that implements an ISMS.

Effectively, therefore, what one would be doing is extending an existing management system to include information security management, not bringing in a whole new system. This is an important message that should underpin the organisation's change management and communication plans; the smaller the perceived mountain, the more quickly will an organisation set out to climb it.

In circumstances where the organisation does not already have an existing ISO9000 certified management system and wishes for guidance on the documentation and document control and records issues of ISO27001, it should obtain, and use, the guidance in any current manual on the implementation of ISO9000.

It is also important that the assessment and certification body chosen by the organisation understands and accepts this integrated approach. If it does not, get a new one; the task of having the existing system re-assessed (and only at the next planned surveillance date) is much smaller than the task of creating and implementing a wholly new and parallel ISMS.

**Project management**

I discussed, in *Chapter Two*, the role of the top level management steering group. In smaller organisations, this steering group will also be the project group. In larger organisations, the steering group will appoint a project

group to deal with the day-to-day implementation of the ISMS.

This project group, or team, should be drawn from those parts of the organisation most likely to be affected by the implementation of the ISMS, as well as a very small number of functional experts, including HR/personnel. The balance is important; a properly functioning ISMS depends on everyone in the business understanding and applying its controls and, if the project team is made up of a preponderance of non-technical people, it is more likely to produce something that everyone in the business understands. The team certainly should include at least one experienced project manager, who will be responsible for tracking and reporting progress against the planned objectives. The project team should report directly to either the chairman of the steering group or (preferably) the CEO, and should have the appropriate delegated authority to implement a board-approved ISMS project plan. Clause 7.2 of ISO27001 requires the provision of adequate and competent resources to establish the ISMS, and putting an appropriately structured project team in place is the first step in doing this.

Project team members should be selected from across the organisation. Members should be in senior positions within the organisation. Key functions that should be represented are quality/process management, human resources, training, IT and facilities management as they will all have to change their working practices significantly as a result of the decision to implement an ISMS. Apart from the manager responsible for information security and a trained information security expert, the most critical representation will be from sales, operations and administration. These tend to be the functions in which the majority of the

organisation's personnel are employed, and the ones that will be most affected by the implementation of an ISMS. Ideally, the people invited to represent these functions should be amongst the most senior and widely respected individuals within them.

As mentioned earlier in this book, the change process that ISO27001 implementation will require has a cultural impact. It is critical that those most able to represent, and articulate, the needs and concerns of the key parts of the organisation are included on the working party. Without their involvement, there is unlikely to be the 'buy-in' necessary for the ISMS to be effectively developed and implemented.

***Project team chair***

The choice of chairman for the project team is usually critical to its success, both as a group, and in terms of how the rest of the organisation views and responds to it. The chairman needs, therefore, to be someone who is capable of commanding the respect of all members of the project team. S/he needs to be wholly committed to achieving the goal of a certified ISMS, within the board-agreed timetable. S/he needs to be pragmatic and prepared to 'think outside the box' in identifying solutions to organisational problems that are affecting implementation.

This person should not be from any one of the organisation's support functions as this will usually brand the project as an unimportant one. It should, on no account, be led by an IT person, as the implementation of an ISMS simply cannot afford to be seen as only an IT project. S/he should, preferably, have a broad managerial responsibility within the organisation, as well as experience in

implementing cross-organisational change projects. Ideally, s/he will be the chief executive or the main board director who has been charged with implementation of the Board's security policy.

In smaller organisations, this person might also be the manager responsible for information security; in larger organisations, where this is likely to be a full-time role, the manager responsible for information security should properly report to the chairman of the steering group, or the CEO.

Not only is the structure outlined here the most effective method for delivery of the ISMS, it is also very clear evidence of commitment from the very top of the organisation, to its implementation. The external ISO27001 auditor will expect to see such evidence.

**Project plan**

Normal project planning tools should be deployed in creating and managing the ISMS project. The project plan needs to contain an outline timetable and a top level identification of responsibilities, as well as the critical path to completion. This plan should be prepared by the project team and, once it has been critically tested by the CEO and top management, approved by the Board. This plan has to be capable of being understood by the senior management and board, and should, therefore, be capable of appearing on two sides of A4. It should also provide sufficient scope, for those who will have to implement the plan, to find appropriate solutions to the many operational challenges that there will be. It should not, in other words, be a detailed plan – although the thinking behind it should be detailed.

A key preliminary step in any successful change programme is to identify and isolate, or convert, potential opposition. Where an ISMS roll out is concerned, there is sometimes internal resistance from within the IT department. There are a number of possible reasons for this, including the desire of the Head of IT not to lose control of IT security (particularly where ISO27001 accreditation has been set as an IT department responsibility), the IT department's desire to maintain its mystique, and the fear that its existing controls might be found to be inadequate. This is not surprising. However, ISO27001 does require the organisation's board and senior management to take control of its ISMS, and the whole organisation to get behind, and understand, key aspects of security policy. The resistance of the IT department can sometimes be expected, and must be overcome at the outset. There are circumstances where this can lead to a change in IT staff, either forced or unforced, and the organisation should expect this and prepare appropriate contingency plans.

Training will be an important facilitator of the change programme. The project team will need initial training in the principles of ISO27001, the methodology of change and project management, and the principles of internal communication. Staff throughout the business will need specific training in those aspects of security policy that will affect their day-to-day work. The IT manager and IT staff will all need specific competences in information security (*see ISO27001 clause 7.2*) and, if this needs to be enhanced by training, this should be delivered by an organisation that recognises, and understands, the technical aspects of ISO27001 training. More information about appropriate training is here: *www.itgovernance.co.uk/training.aspx*.

## Costs and project monitoring

There should, at this stage, also be an estimate of the costs and resources involved in implementing the ISMS, an assessment and quantification of the potential benefits, and an outline implementation plan that describes, at the top level, who will be responsible for doing what, and by when. Such a document should be prepared and presented to the Board, along with the proposed security policy. This document should set out clearly the proposed dates at which the Board will be invited to review progress towards final implementation so that it can ensure that the information security policy is being properly implemented.

Every organisation has its own preferred format for presenting project initiation documents or project proposals, and you should use whatever is normal for your organisation. A key recommendation, however, is that review dates should be realistically spaced and that the plan should allow executive management sufficient flexibility in implementing a policy that will have to be designed in the light of facts that may not be known at the point at which the policy is adopted.

The key points for project progress review are:

- After completion of the draft statement **of** applicability (SoA). Any costs incurred prior to this should be minimal but, until the SoA defines what needs to be done, it will not be possible to budget effectively for the implementation.
- After implementation of the initial suite of procedures that apply the identified controls.
- After completion of the first cycle of system audits and reviews, and prior to the initial visit by the certification body.

- Annually, as part of the regular review of the ISMS, to ensure that the budget is being correctly applied and that any new technology issues, threats or vulnerabilities have been taken care of.

It is assumed that the organisation already has well-developed procedures for dealing with projects that are missing key review dates, and in which there is overspending or underperformance. This book does not, therefore, make any proposals about what action should be taken to rectify shortfalls, but will make the observation that early and vigorous action by the Board will go a long way to proving to the organisation the seriousness of the endeavour and, thus, to bring about the achievement of certification.

**Consultants**

There are strong arguments both for, and against, the use of consultants in any ISMS project. There are two essential arguments in favour of bringing in outside consultants:

1 They already possess the expertise and knowledge necessary to successfully deploy an ISMS.
2 Your existing resources are inadequate for the demands of the ISMS project and need short-term strengthening.

There are also two essential arguments against bringing in outside consultants:

1 Consultants are an expensive drain on resources, not just in terms of their own costs, but in terms of the additional work they almost always identify that absolutely has to be done (by someone other than you – usually themselves).

2 You need to have the information security management skills, and the knowledge of how to make information security work for your organisation, deeply embedded in your organisation. The only really effective way to ensure this happens is to manage and resource the implementation of your ISMS internally and, in the process of doing so, to ensure that information security becomes part of the fabric of the organisation. Incidentally, this is also what the Standard is looking for, not least because experience teaches that this is fundamental to a long-lasting information security culture.

We recognise 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 organisation tackles change projects. In those organisations that have a history of using – and successfully using – consultants to facilitate change, the argument in favour of using ISMS consultants is balanced more towards using them than not.

In organisations that do not have any deep experience in managing consultants, or those 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 – unless it is on the basis of what we would call a mentor and coach approach, which involves providing extensive guidance and support for your internal ISMS team, such that the ISMS is quickly and effectively implemented, and they gain the necessary skills and knowledge to maintain it in future.

The reason for this is simple: consultants, like any other organisational resource, have to be managed. Previous organisational 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 sensitivity, and a great deal of leadership. No consultant is able to provide organisational leadership, although many may – in a vacuum – try. 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.

- You can use consultants – trusted third parties – to communicate the seriousness of the information risks faced by the organisation and the need, therefore, for an ISMS – remembering that any such communication will always be more effective if it is well understood throughout the organisation that the consultants are not getting any further work out of frightening everyone.
- You can use consultants to provide advice on specific (most often technical) issues – related, for instance, to scoping, and how external or internal threats might affect your decisions about project scope, or to carry out a risk assessment, or to deal with documentation, to advise on integration with other management systems, etc.

- You can (and might be well-advised to) use consultants to help you identify appropriate technical controls for specific risks that you have identified – as long as the consultants have no financial interest in any solutions they might recommend and fully understand and can help you apply the two key financial measures of return on investment (ROI) and total cost of ownership (TCO) to any solutions they propose.
- You can use consultants in a mentoring capacity to review critical documents, and as a sounding board with whom you can discuss key steps in your project, key issues that you have to deal with, and possible solutions.

However you decide to proceed, you need to clearly make your decision as to how you are going to proceed relatively early in your project, so that you can make appropriate staffing, resourcing, managerial and financial decisions. More information about consultancy is available here: *www.itgovernance.co.uk/iso27001_consultancy.aspx*.

**Information security manager**

Whatever decision you make about the use of consultants, you will need to appoint an information security manager. It is good sense for, and ISO27001 expects that, one manager will be made responsible for all security-related activities – both strategic and day to day – within the organisation. This person could be appointed before the steering group and/or project team is set up, and his/her brief could include the formation of the steering group and/or project team. The benefit in this route is one of speed and, potentially, of simplicity. The board member who has been charged with the responsibility for ensuring implementation of the ISMS could simply select and

appoint an appropriate person, who could then get on with putting together an appropriate project team, which could then take things forward. The selection and training of the members of the steering group is potentially more time consuming, and the period during which they are learning their roles will precede the point at which they are competent to select and appoint an appropriate manager. The organisation may not wish to pursue this slower route.

While the information security manager does not need to be the same person who is appointed as the organisation's information security expert (the skill sets required for the managerial role, particularly in a larger organisation, may be different from those required for the security expert's role), this person will still need adequate training in information security matters. Obviously, the person selected for the managerial role will need to be an effective manager, with well-developed communications and project management skills.

### *Specialist information security advice*

Information security has a number of technical aspects and many technical considerations must be taken into account when designing and implementing an ISMS. This does not mean, as I have said before, that the project should be led by a technologist, or that it should have anything other than a complete business focus. The organisation does need to have available to it a source of specialist information security advice, who can provide – on an ongoing basis – detailed input of information security threats, on appropriate control configurations, and on reliable monitoring and auditing processes. This role can be difficult to fill on a part-time basis – you want your specialist to have a working and detailed knowledge of your

organisation – but not all organisations can afford a full-time resource. This leaves two alternatives, both of which involve substantial training: appoint someone from within the IT team to the role, and ensure s/he gets adequately trained on the information security issues, or appoint someone from elsewhere (possibly, in a small organisation the information security manager), and ensure s/he has adequate technical training and depth of know-how. The choice between the two options will be a pragmatic one, informed by the characters, attributes, and personal circumstances of the potential candidates.

In larger organisations, of course, the recruitment and appointment of such an expert should be a matter of priority, if it hasn't already happened. The one issue to which such a person is unlikely to have had adequate exposure is the information security management Standard, and, therefore, steps should be taken to provide this person with specific ISMS training – such as that provided by an IBITGQ ATO (accredited training organisation).

### *Functional specialists*

There are a number of functional specialists who will need to be involved in the project and whose contributions will need to be effectively inspired and coordinated. These people include the leaders of the IT unit, the Head of HR, the risk assessment or risk management experts within the organisation, the premises security people, and both the finance and internal audit teams. It is worth seeking their early involvement, both by including them in the initial round of briefings on the need for an information security management system, eliciting their views as to risks and threats, and considering their likely critical contributions.

While you should involve them early on – because, with them, you will succeed whereas, without them, you are almost certain to fail – you should keep clearly in mind – and make sure they fully understand – that this is a business project, which will be led by, and reflect the needs of, the business.

# CHAPTER 5: COMMUNICATION

The same rule that once applied to voting in elections, also applies to communication in change programmes: 'communicate early and communicate often'. Communication is so important that it is one of the nine keys to ISO27001 project success. Underlying every successful change management programme, and especially necessary for the successful roll out of an ISMS, is a well-designed and effectively implemented internal communications plan. Compliance with ISO27001 and common sense suggests that key components of this plan must include:

- Top-down communication of the information security vision – why the ISMS is necessary, what the organisation's legal responsibilities are, what the business will look like when the programme is complete, and what benefits it will bring to everyone in the organisation.
- Regular cascade briefings to all staff on progress against implementation plan objectives. These briefings should quickly become part of the existing organisational briefing cycle, so that ISMS progress becomes part of the normal business process – 'just another thing that we're doing'.
- A mechanism for ensuring that key constituencies and individuals within the business are consulted and involved in the development of key components of the system. This ensures that they buy in to the outcome and to its implementation, and is a key reason for

structuring the steering group and project team, as was suggested in *Chapter Two*.

- A mechanism for ensuring regular and immediate feedback from people in the organisation, or in affected third party organisations, so that their direct experience of the initial system as it is implemented can be used in the evolution of the final version. This can form part of your continuous improvement process and, more immediately, offer evidence of effective 'checking'.

These face-to-face communications should be underpinned with an effective information sharing system. Most usually, this will be part of the corporate intranet, on which regular progress reports, as well as detailed information on specific aspects of the ISMS, are posted. E-mail alerts can tell staff to access the intranet for new information whenever it is posted and the site can encourage feedback by means of a 'write to the CEO' function.

Of course, if the organisation doesn't currently have a well-developed internal communication process, it will need to develop one. Allowance should be made in the outline project planning timetable and there should be resource allocation for the development of such a system. Do not try and take an ISMS project forward without an adequate internal communication process: information security controls depend, to a very large extent, on the informed and committed behaviour of individuals within the organisation and, as a result, you simply have to ensure that you can deliver this.

### Staff buy-in

The initial staff briefing, the one that accompanies the project kick-off, should set out, clearly, the nature of the

threats faced by the organisation and the possible costs, in both financial and non-financial terms, of information security breaches. *The Case for ISO27001:2013* (available from *www.itgovernance.co.uk*) provides a well-argued case for the need to deploy an ISMS, and the information provided in that book can be used for your staff communication. The book is also a useful tool for getting buy-in from senior management, and from across the organisation; organisations that have distributed a number of copies of *The Case for ISO27001:2013* amongst senior managers – both line of business and functional – have made more rapid progress toward developing an organisation-specific vision of what the ISMS should like, what the risks are that have to be controlled, and what the benefits of deployment will be.

Wherever possible, though, local and/or industry specific information should additionally be sought and used in staff presentations, as this gives immediacy and currency to the possible threats. Illustrations of the possible direct consequences to your own organisation should be developed, in order to dramatise and help all those involved to fully appreciate the need for the ISMS.

A key part of getting effective user buy-in is translating information security risks and technology issues into widely, and clearly, understood business ones. Boards and managements understand issues in terms of their impact on the business and, unless those impacts are clearly delineated, clearly credible and clearly quantified, they are not going to pay them much attention. The same is true of functional and business leaders across the organisation whose interest is, if anything, more parochially focused on their own specific issues. The truth is that they are less interested in the long-term strategic needs of the

organisation than they are in achieving the specific sets of goals that drive their own compensation or promotion possibilities.

All this means that you not only need to translate the information security imperatives into a small number of credible, quantified and relevant numbers for the Board and senior management, you also need to make the ISMS initiative directly relevant to every single person on whose support you are going to rely. Like all organisational politics, there is almost certainly no one message that will do this job for everyone. You are going to need a single, strong organisation-wide, top-down commitment, supported by a large number of one-on-one, locally focused discussions in which you set out how the ISMS project will specifically improve the business circumstances for each person to whom you talk.

A large part of effective project management is about sales skills and a detailed understanding of the organisational politics; this is why it can be very hard for an outsider to succeed as project manager in delivering an ISMS project.

**Information security policy**

The extent to which you have succeeded in building cross-organisational and cross-functional support for this project will be reflected in the ease with which you are able to get your information security policy drafted and agreed. This information security policy is the main driving force for the ISMS; it sets out the Board's policy on, and requirements in respect of, information security. It should be a short document, but it has to capture board requirements, organisational reality, and meet the requirements of the Standard. It should also include a full discussion of the

issues involved in, and development process required for, an information security policy statement.

'The Board and management' have to be completely behind, and committed to, the ISMS; therefore, the policy statement must be issued under their authority and there should be clear evidence, in the form of written board minutes, that the policy was debated and agreed, both by the Board as a whole, and by the management steering group. Any revisions to the policy should also be debated and agreed by both the Board and the steering group.

It will also require participation by all employees in the organisation, and may require participation from customers, suppliers, shareholders and other third parties. This is part of the context of the ISMS referred to earlier. In thinking through the security policy, the Board and the forum will need to consider how it will impact on these constituents and/or audiences, and the benefits and disadvantages that the business will experience as a result of this. It is a good idea to start thinking these issues through before you commence the detailed process of designing and deploying your ISMS.

# CHAPTER 6: RISK ASSESSMENT

Risk assessment is at the heart of the ISMS. Understanding its significance to the overall process is critical, and is one of the keys to project success. The Board adopts an information security policy because there are a number of significant risks to the availability, confidentiality and integrity of the organisation's information, and it mandates the design and deployment of an ISMS in order to ensure that its policy is systematically and comprehensively implemented. The policy must, therefore, reflect the Board's assessment of information security risks and opportunities. This doesn't mean the Board needs to carry out a detailed risk assessment itself, but it does need to set out a clear, overall approach to risk that can be used to take forward the ISMS project.

The organisation needs, in other words, to determine its criteria for accepting risks, and identify the levels of risk it will accept. It is a truism to point out that there is a relationship between the levels of risk and reward in any business. Most businesses, particularly those subject to Turnbull, will want to be very clear about which risks they will accept and which they won't, the extent to which they will accept risks and how they wish to control them. Management needs to specify its approach, in general and in particular, so that the business can be managed within that context.

Information risk is one of a number of risks that the organisation must control and it should, to the greatest extent possible, apply a common risk management framework to all the risks with which it is faced. The

starting point for any ISMS project manager's consideration of risk is to embrace the existing risk management function (if there is one) inside the organisation, in order to understand a) its overall approach to risk and b) its specific approach to information security risk. If the organisation doesn't have any such formal function, it is imperative that the current approach to identifying, assessing and controlling risk – and those involved in the activity – is identified as quickly as possible. You will need to ensure that there is a consistent, organisation-wide approach to managing the information security risks.

**Introduction to risk management**

All organisations face risks of one sort or another on a daily basis. Risk management is a discipline for dealing with non-speculative risks, those risks from which only a loss can occur. Speculative risks, on the other hand, those from which either a profit or a loss can occur, are the subject of the organisation's business strategy, whereas non-speculative risks, those risks which can reduce the value of the assets with which the organisation undertakes its speculative activity, are (usually) the subject of a risk management plan. These are sometimes called permanent and 'pure' risks, in order to differentiate them from the crisis and speculative types. Usually, the identification of a risk as either speculative or permanent, reflects the organisation's risk appetite.

Risk management plans have four, linked, objectives, which are to:

1 Eliminate risks.
2 Reduce those risks that can't be eliminated to 'acceptable' levels; and then to either

3 Live with them, exercising carefully the controls that keep them 'acceptable'; or
4 Transfer them, by means of insurance, to some other organisation.

Pure, permanent risks are usually identifiable in economic terms; they have a financially measurable potential impact upon the assets of the organisation. Risk management strategies are usually, therefore, based on an assessment of the economic benefits that the organisation can derive from an investment in a particular control; in other words, for every control that the organisation might implement, the calculation is that the cost of implementation should be outweighed by the economic benefits that derive from, or economic losses that are avoided as a result of, its implementation.

The organisation should define its criteria for accepting risks (for example, it might say that it will accept any risk whose economic impact is less than the cost of controlling it) and for controlling risks (for example, it might say that any risk that has both a high likelihood and a high impact must be controlled to an identified level, or threshold).

This chapter only provides a brief introduction to, and overview of, risk management. There is more detailed guidance on this process in *Information Security Risk Management for ISO27001/ISO27002*.

The ISO27001 requirement is that the risk assessment should take into account both the organisation's context (internal and external), as well as the requirements of third parties that might be relevant to, or have an interest in, the organisation's approach to information security. The previous version of the Standard spoke of taking into account the business, legal and regulatory requirements

placed on the business. In other words, the risk assessment must be business-driven and must reflect legal, regulatory and contractual requirements. This is one of the most important ideas in information security: the business, managed by its board of directors, should identify the threats to assets, vulnerabilities and impacts on the organisation, and should determine the degree of risk that it is prepared to accept – in the light of its business model, business strategy and investment criteria.

**Baseline control set**

The first step in the process is to identify and implement the controls that would be required in order to meet the organisation's legal, regulatory and contractual obligations (and there might be a number of different obligations, depending on jurisdictions within which it operates). It is also necessary to identify any controls that might be required by customers, or suppliers, or other contractual mandates, and to include them in the baseline control set. Deployment of a compliance database (e.g. *www.itgovernance.co.uk/shop/p-715-iso27001-compliance-database-and-update-service.aspx*), which enables specific identification of controls in relation to specific legal requirements, can be an effective way to tackle this first step.

The second step in the process is to identify those additional controls that might be required to control risks other than those arising from a failure to meet legal, regulatory or contractual obligations.

## Risk assessment

Risk assessment is defined in ISO27000 as a process that combines risk analysis and risk evaluation. Risk analysis is the 'systematic use of information to estimate risk', and risk evaluation is the 'process of comparing the estimated risk against given risk criteria to determine its significance'.

In simpler terms, risk assessment is the systematic and methodical consideration of: a) the realistic likelihood of a risk occurring and b) the business harm likely to result from any such risks.

The risk assessment should be a formal process. In other words, the process should be planned and the input data, its analysis and the results should all be recorded. 'Formal' does not mean that technical risk assessment tools must be used although, in more complex situations, they are likely to improve the process and add significant value. The complexity of the risk assessment will depend on the complexity of the organisation, and of the risks under review. The techniques employed to carry it out should be consistent with this complexity and the level of assurance required by the Board.

### *Who conducts the risk assessment?*

Unless the organisation 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 organisation) need to delegate the responsibility to a lead risk assessor. There are two ways of doing this. The first is to hire an external consultant (or company 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 organisation already has a trained information security adviser, this person could take on the role.

In circumstances where the organisation 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 3, 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'. The risk assessment process should also allow for the possibility of unexpected positive outcomes, or what the Standard calls 'opportunities'. Risks are analysed in terms of their likelihood of occurrence, and their impact if they do. The impact can be either positive or negative. Different organisations have different thresholds in terms of what they consider acceptable – what they can live with – in terms of likelihood and impact, and this threshold must be defined in terms of risk acceptance criteria.

**Risk workshop**

The most effective way to perform the risk assessment (having first defined and documented the risk assessment

process) is to hold a risk workshop. The starting point for this workshop would be for the lead risk assessor to create a list of relevant risks that would compromise the confidentiality, integrity and availability of information that is within the scope of the management system, and which roles within the organisation might own each of those risks.

The risk workshop would be convened and managed by the lead risk assessor and would involve all the risk owners from across the business. The role of the risk workshop is to ensure that the list of identified risks (and relevant opportunities) is complete, that risk owners have been appropriately assigned to determine the likelihood and impact of each of the identified risks, and to evaluate those risks against the identified risk acceptance criteria.

**Impacts**

Identify the possible impacts that the occurrence of a risk event will have on an information asset's availability, confidentiality or integrity (impact analysis). These impacts should all, wherever possible, be assigned an estimated monetary value, using a category system (e.g. less than £1k, between £1k and £10k, etc.) that reflects the size of the organisation, and the total cost (direct and indirect) of the incident.

Assess the probability of the event occurring, using a classification system such as once every few years, once per year, once every six months, etc. Virus attacks would fall into the everyday category.

This then enables one to identify the level of risk (and, pragmatically, a low–medium–high classification is usually adequate for a smaller organisation) and then to conclude, for each risk, and in the light of controls already in place,

whether it is acceptable, or if some form of additional control is required.

## Controls

Your risk assessment drives your selection of controls, over and above those that might fall within, what I have called the 'baseline control set'. The key thing to bear in mind about the risk assessment is that it is not a once-only exercise. You will need to repeat it on a regular basis, just to check that your baseline assessment is still accurate and that the controls you have deployed are still appropriate. You will need to carry out specific risk assessments on an ongoing basis whenever there is a change in circumstances or in business structure or environment, or in the risk profile. Every decision you make about the controls that you are going to deploy must be driven by your risk assessment.

Therefore, your approach to risk assessment will be a cornerstone of your ISMS. That is why many organisations use risk assessment tools as part of their management system.

## Risk assessment tools

There are a small number of software tools available that can, to one extent or another, automate the risk assessment process. Some can generate the statement of applicability, although not all of those that do this will give you something that is actually useful. In theory, a risk assessment tool ought to encourage the user to perform a thorough and comprehensive security audit on the organisation's information systems, and ought not to produce too much paperwork as a result. Any organisation

interested in pursuing this route should do up-to-date research on what is available, before making a shortlist.

The organisation will need to compare tools before making a selection and should concentrate, in the comparison process, on the extent to which the tool really does easily and effectively automate the risk assessment process, the amount of additional paperwork it generates, the flexibility it offers for dealing with changing circumstances and frequent, smaller scale risk assessments, and the meaningfulness of the results it generates. Of course, normal due diligence should also be factored into the status of the supplier and manufacturer of the product, to ensure that it is properly supported and likely to continue to be supported.

Risk assessments can be done without using such tools. A thorough risk assessment of any significant business will be very time consuming, whether or not a software tool is used. ‘Time consuming’ means up to a month and, for larger organisations, even longer. The use of a software tool will depend on the culture of the organisation, and the preferences of the information security adviser and the ISMS project manager.

# CHAPTER 7: CONTROL SELECTION

The risk assessment is at the heart of the ISMS. The controls adopted by the organisation will form a significant part of the ISMS. The reality is that the bulk of the project time will be invested in designing, deploying, testing and revising appropriate controls that are intended to meet the identified risks. It is therefore important to have an overview of controls.

The concepts of risks and controls are linked and are fundamental to Information Security Management Systems. Risk might be defined as 'the combination of the probability of an event and its consequences'. Control is defined, in ISO/IEC 27000, as the 'means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management or legal nature; [the word is] also used as a synonym for safeguard or countermeasure'. Please note that information security controls are not simply technical in nature. If they were simply technical, they would fail – even if only because no control can implement and maintain itself autonomously.

## Nature of controls

All information security controls are made up of a mix of process/procedure, technology and human activity. Looking, for example, at the virus and cyber threats that are widely recognised, even by boards of directors, ISO27001 Control A.12.2.1 – and common sense – requires the implementation of controls against malicious software and, when you think about this issue, it is immediately clear that

technological controls must be blended with procedural ones – neither on its own is adequate. It is also clear that malware that corrupts a system is not only a business continuity and reputational issue – it may also corrupt records that need to be retained, or make it impossible for an organisation to complete or submit required reports on time.

At the same time, ISO27001 Control A.13.2.3 requires that information 'involved in electronic messaging should be appropriately protected'. Anti-malware software, on its own, just doesn't meet a requirement which clearly covers both e-mail and instant messaging. What you need, according to both common sense and ISO27001, is a mix of technology, process and correct behaviour.

Yes, you need an appropriate software package, one that will ensure that incoming viruses, worms and Trojans are stopped at the perimeter – and that spam is filtered out – but it is no good if documents that users have specifically requested from external sources, and which are coming by e-mail, are corrupted by the anti-malware software 'just in case' – we know, for instance, that PDFs sent via an automatic response e-marketer are often nuked by the recipient organisation's anti-malware software, and that the same document, when sent individually to the recipient, will pass through with little problem – this sort of software set-up promotes disrespect amongst its users and a tendency to try and bypass it – potentially with attachments that are really dangerous. Instant messaging has become one of the simplest ways for individuals to circumvent e-mail restrictions and ISO27001 now expects those risks also to be identified and controlled.

End-point security is now also a huge issue – traditionally, the organisational information security perimeter was easy to define and defend – with the proliferation of handheld devices, wireless networks and mobile working, the perimeter has become very hard to defend, and very porous – so, depending on the risk assessment, organisations need to be looking at software that will tackle the risks in handhelds, rather than making them difficult to deploy. Wireless networks need to be properly set up – and mobile access should be by means of an appropriately secure connection – probably a VPN. This control area will be found to interact with control A.6.2, which requires the organisation to have in place a formal policy and appropriate controls to protect against the risks of working with mobile computing facilities.

Of course, anti-malware software needs to work with the firewall, seamlessly, and it goes out of date – fast – so you need to have in place procedures that ensure it is properly updated. Most organisations don't have a lot of time for testing anti-malware or other updates and fixes. Nevertheless, exploits to attack revealed vulnerabilities are now happening faster and faster – so rapid deployment of fixes is usually critical, and this can only be achieved if you've got the right structures and processes in place.

In addition, your staff need to be trained on what to do when there is an incident – whether an e-mail virus, a hoax, or someone uploading something from a USB stick. When it all goes wrong (as, sooner or later, it inevitably will), you need to have put in place ways of keeping the ship afloat while you fill the holes.

## Control selection criteria

You should only deploy controls that relate to, and are appropriate and in proportion to, the actual risks you face. While you can select controls from any source you consider appropriate, ISO27001:2013 requires that you compare any controls that you do select against the list that it considers to be the key best-practice controls that might be considered in relation to the whole range of potential risks (many of which your organisation may not face), and for inclusions and exclusions to be justified.

Controls can also, more simply, be described as 'the countermeasures for risks'. Apart from knowingly accepting risks that fall within the (board-determined) criteria of acceptability, or transferring those risks (through insurance) to others, there are four types of control:

1 Deterrent controls reduce the likelihood of a deliberate attack.
2 Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
3 Corrective controls reduce the effect of an attack.
4 Detective controls discover attacks and trigger preventative or corrective controls.

Controls, however, are not implemented irrespective of the cost. No board should sign off on any ISMS proposal that seeks to remove all risk from the business – the business does, after all, exist within a risk framework and, as the only form of existence that is completely risk-free involves already being dead, there is little point in proposing to control every risk.

It is essential that any controls that are implemented are cost effective. The principle is that the cost of

implementing and maintaining a control should be no greater than the identified and quantified cost of the impact of the identified threat (or threats). It is not possible to provide total security against every single risk; the trade-off involves providing effective security against most risks.

No organisation should invest in information security technology (hardware or software), or implement information security management processes and procedures, without having carried out an appropriate risk assessment that assures them that:

- The proposed investment (the total cost of the control) is the same as, or less than, the cost of the identified threat's impact.
- The risk classification, which takes into account its probability, is appropriate for the proposed investment.
- The priority of the risk – i.e. all the risks with higher prioritisations have already been adequately controlled and, therefore, it is appropriate now to be investing in controlling this one.

If the organisation cannot satisfy itself that the proposed investment meets these criteria, it will be wasting money – and the time required to implement the control – while leaving itself open to more likely risks and, conceivably, with inadequate resources to respond to the more likely risk when it occurs. There is, in other words, a risk associated with not carrying out – and maintaining – an adequate risk assessment.

**Statement of applicability**

The second most important document in your ISMS – after the information security policy statement itself – is your statement of applicability, or SoA. The SoA is, in essence, a

list of all the controls identified in Annex A of ISO/IEC 27001:2013, together with your statement as to whether or not that control is applied in your organisation, together with a justification for its inclusion or exclusion. Either choice, for or against applying the control, must be justified by the risk assessment (including the baseline controls required to meet legal, regulatory and contractual objectives), and each control must be proportionate to the identified risk.

ISO/IEC 27002 has the status of a code of best practice, and it is the identified, and preferred, resource of ISO/IEC 27001 for detailed information about implementation of the controls listed in ISO/IEC 27001 Annex A (although you should see *Chapter One* for more information on this subject).

The best detailed guidance that exists on the market today, and which tackles the SoA on a control by control basis, is *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*, which was chosen as the Open University's postgraduate textbook, precisely because of the quality of its coverage of this core component of the ISMS. Whether you are using consultants for your project or not, you will find this book indispensable[1] to your ISMS project.

[1] While I am one of the co-authors of this book, the fact is that there is nothing like it on the market.

# CHAPTER 8: DOCUMENTATION

Your risk assessment process determines the controls that have to be deployed in your ISMS, and your statement of applicability identifies the controls that you are deploying in the light of your approach to risk management. Every one of those controls, together with your approach to identifying and managing risk, your management structure, your decision-making processes, and every other component of your Information Security Management System, has to be documented, as a point of reference, as the basis for ensuring that there is consistent application over time, and to enable continuous improvement.

Documentation will be the most time-consuming part of the total project and, therefore, how you decide to tackle this aspect will be a major determinant of your overall success. Documentation has to be complete, comprehensive, in line with the requirements of the Standard, and fit for your organisation like a glove tailored for a hand. A properly managed ISMS will be fully documented. ISO27001 describes the minimum documentation that should be included in the ISMS (to meet the Standard's requirement that the organisation maintain sufficient records to demonstrate compliance with the requirements of the Standard). These documents include:

- The information security policy, the scope statement for the ISMS, the risk assessment, the various control objectives, the statement of applicability and the risk treatment plan. Evidence of the actions undertaken by the organisation, and its management to specify the

scope of the ISMS (the minutes of board and steering committee meetings, as well as any specialist reports).

- A description of the management framework (steering committee, etc.). This could usefully be related to an organisational structure chart.
- The risk treatment plan and the underpinning, documented procedures (which should include responsibilities and required actions) that implement each of the specified controls. A procedure describes who has to do what, under what conditions, or by when, and how. These procedures (there would probably be one for each of the implemented controls) would be part of the policy manual which, itself, can be on paper or electronic.
- The procedures (which should include responsibilities and required actions) that govern the management and review of the ISMS.

All formal documentation should be controlled and available to all staff who are entitled to view it. It can be published in paper form but is most effective on an intranet, a shared drive or SharePoint. An intranet ensures that the current version of any procedure is immediately available to all members of staff, without hassle. A structured numbering system should be adopted that ensures ease of navigation of the documentation, and also ensures that document issue is controlled, that replacement pages and changes are tracked, and that the documentation is complete. Staff should be trained in how to use the documentation and staff will also need to be trained in how to draft operations procedures for the assets and processes for which they are personally responsible.

Clearly, there will be a number of security system documents which will need to be subject to security measures. These will include documents such as the risk assessment, the risk treatment plan and the statement of applicability, which contain important insights into how security is managed and which should, therefore, be classified and restricted and treated in accordance with the organisation's information classification system. Access should be limited to people with specified ISMS roles, such as the information security adviser.

**Four levels of documentation**

ISO27001 clearly recognises that there is no such thing as a 'one size fits all' approach to documentation. Instead, it recommends that the extent of the ISMS documentation should reflect the complexity of the organisation and its security requirements. In practical terms, there are four levels of documentation in an ISMS, and each level has different characteristics, including about who is entitled to make decisions regarding revisions to them. The four levels are:

1 The Board-approved corporate policy, which drives all other aspects of the ISMS. This high-level policy is supported by a small number of additional, subject-specific policies (setting out, for instance, what constitutes acceptable use of the Internet).
2 Detailed procedures, that describe who is responsible for doing what, when and in what order.
3 Operations/work instructions, that set out in detail precisely how each of the identified tasks are performed.
4 Records, which provide evidence as to what was done.

The amount of work increases as you descend the four levels; the most demanding, in terms of time, is producing the third level – even though this is essentially the documentation of existing ways of carrying out specific activities – once, of course, those have been brought into line with the control requirements.

## Documentation approaches

There are three approaches to tackling the documentation requirements of the Standard, two traditional and one using a documentation toolkit. In an organisation that meets the criteria described earlier in this book, the length of time that the project will require will depend very much on the methodology adopted.

### *Trial and error*

The first is a methodology known as 'trial and error' and, because those charged with deploying the ISMS first have to learn how to perform every single aspect of the task, it is the most time-consuming of the three, has a high risk of failure, and extends the period during which the organisation continues failing to meet its information security objectives.

### *External expertise*

The second, equally traditional, method is to bring in outside expertise in the form of experienced consultants. The pros and cons of such an approach were discussed in *Chapter Four*. It is a quicker approach than the trial and error one, but is substantially more expensive. Its major advantages include considerably reducing project time, reducing the risk of failure, increasing the speed of

organisational learning, and overcoming resource deficiencies.

***Third party documentation toolkit plus guidance***

While this approach is most appropriate for organisations that prefer to tackle internal change projects largely without external consultant support, it is an approach that depends for its success as much on the quality and extent of senior management support and commitment, as it does on the quality of the tools themselves.

The major advantages of this approach are that documentation toolkits are:

1 Fit for purpose – designed to meet ISO27001 requirements from the outset.
2 Fast to deploy.
3 Very cost effective (with low TCO and high ROI).
4 Generate substantial cost savings in comparison to traditional approaches.
5 Full of best practice.
6 Will be cross-functional, company-wide, with correct continual improvement cycle.
7 Very low likelihood of project failure.
8 Continuous improvement built in from the start.

It is essential that any documentation toolkit be designed to meet the detailed requirements of the Standard, and that it comes with detailed guidance on how to tackle the project and all of the detailed drafting requirements. At IT Governance, we design and build a documentation toolkit that exactly meets the requirements of the Standard, which reflects multiple successful deployments of certifiable Information Security Management Systems, and which was

developed specifically for organisations that want to avoid the costs and disadvantages of learning by trial and error.

There is a free, trial version of this toolkit available for download through *www.itgovernance.co.uk*. It is worth checking this toolkit out as part of your preparatory research into how you are going to tackle the documentation part of your project.

# CHAPTER 9: TESTING

The ninth and final key to a successful ISMS implementation is testing – and testing everything to destruction. The principle is a simple one; so simple, in fact, that this will be the shortest of all the chapters in this book.

Your ISMS has to work in the real world. You've identified risks, you've deployed what appear to be appropriate controls, and you want to be sure of two things: first, that the controls work as intended and, second, that when they are overwhelmed (as, sooner or later, they will be) your emergency countermeasures also work. Your management system, including each and every control, is planned and deployed, the management system and every control is then tested to see they work according to plan, and the management system and every control is improved in the light of that testing.

There are four types of testing that should be considered. The first is a straightforward audit, which involves a trained ISMS auditor taking a documented procedure and asking for evidence that what is described in the procedure is what actually happens. As part of your ISMS project, you will need to put in place a team of trained ISMS internal auditors. These people can be drawn from around the business, appropriately trained and, provided you ensure that they never audit any part of the business for which they – or their managers – are responsible, they will meet your long-term audit team requirements.

The second is a limited 'paper test'. This is an intellectual exercise that requires more than one person, and which

requires familiarity with the vulnerabilities in the asset, the mechanisms of the control, and the mechanisms and make-up of the likely threats. Given this knowledge, which should be current, as well as experientially and technically based, the effectiveness of controls (such as incident management or business continuity controls) can be logically tested.

The third is a limited, real-life test. This, for instance, would involve powering down the server room during normal operations, to find out whether the APS systems and server shut-down procedures all worked as specified. Real-life tests should not be carried out without first having taken extensive steps to ensure that, if something doesn't work as planned, the system can be restored to the point it was at when the test was executed. This type of testing includes penetration testing, which should be carried out by a specialist penetration testing company, and should be both testing your selected controls, as well as your risk assessment: in other words, you should instruct your penetration tester to try and penetrate your system by methods that you haven't identified. You can later assess whether these are threats against which you need to control.

The fourth and final type of test is a large-scale scenario test, most usually used to test business continuity plans. These tests usually try and telescope the events of several days into a much shorter space of time and require all those who would have roles in the real-life disaster to attempt to perform the required tasks in the role play. These tests require considerable planning and it is a sensible area in which to deploy external, specialist expertise.

You will need to schedule audits and tests so that, in the course of a year, all aspects of your ISMS are covered. You

will need to do this on the basis that some controls will need to be tested more regularly than others; you should carry out a risk assessment to determine the frequency of testing that you will require. Your external certification auditors will want to see evidence of your internal audit and testing, the results of this activity, and details of how you have used the findings of this activity to improve and tighten your ISMS. You should assume that your external certification auditor will want to see evidence of at least one cycle of audits and tests. If you want to achieve certification after less than one year's worth of testing, you will need to design a test and audit cycle that covers all the mission critical aspects of your ISMS within a much shorter time-frame. This is not an unusual approach, and most certification bodies should accept that there are a number of items that do not need to be tested that regularly.

# CHAPTER 10: SUCCESSFUL CERTIFICATION

While your selection of certification body should have no impact on your success in achieving certification, there are a couple of issues you should consider in making your selection – which isn't necessary until you have already made considerable progress toward readiness for certification. You will, of course, want to ensure that there is a cultural fit between yourself and your supplier of certification services, and that pricing, etc. is acceptable.

There are two other key issues that do need to be taken into account when making this selection: the first is relevant to organisations that already have one or more externally certified management systems in place; and the second applies specifically to organisations tackling ISO27001.

It is essential that your ISMS is fully integrated into your organisation; it will not work effectively if it is a separate management system and exists outside of, and parallel to, any other management systems. Logically, this means that the framework, processes and controls of the ISMS must, to the greatest extent possible, be integrated with, for instance, your ISO9001 quality system. Clearly, therefore, assessment of your management systems must also be integrated: you only want one audit that deals with all the aspects of your management system. It is simply too disruptive of the organisation, too costly and too destructive of good business practice, to do anything else. You should ensure that whoever you choose for your ISMS audit can, and does, offer an integrated assessment service.

The second issue that you should take into account when selecting your supplier of certification services is their

approach to certification itself. An ISMS is fundamentally designed to reflect the organisation's assessment of risks in and around information security. In other words, each ISMS will be different. It is important, therefore, that each external assessment of an ISMS takes that difference into account, so that the client gets an assessment that adds value to its business, rather than one that is merely a mechanical comparison of the ISMS against the requirements of ISO27001.

There are, once you have chosen your certification body, and once you are ready for a certification audit, six secrets to certification success. None of these secrets will get you through an audit that you are fundamentally not ready for, nor will they enable an inadequate ISMS to achieve certification. What they do do, is ensure that all the good aspects of your ISMS are noted, and that the overall impression with which the auditors are left is a favourable one.

1 Ensure that your documentation is complete, comprehensive and all available for inspection – at the initial visit, the one that comes before the actual certification audit. This first visit is expressly to determine if your ISMS is ready for external audit; impress the auditors as early as possible.
2 Ensure that all your internal audit and testing records are immediately available for the certification auditors when they plan and commence their work; they should use these records to ensure they focus on key areas of the ISMS, so ensure that you have adequately tested them. No external auditor wants to 'sign off' a system that is breached a week later, and the thoroughness of your own work will give the auditor confidence.

3 Teach staff throughout the organisation to be completely open and honest with the auditors, especially about things which they feel may not be up to standard. This serves two purposes: it flushes out weaknesses that you can tighten up on, and it demonstrates to the auditors that you have an open organisation that identifies, and deals with, information security issues. Any attempt to suggest that everything throughout the organisation is perfect, on the other hand, will provoke incredulity amongst the auditors; they have learned, through long experience, that not only is everything never perfect, but that every attempt to pretend to perfection hides a myriad of previously undetected imperfections. Do not encourage them to start hunting these imperfections down.
4 Teach those staff who are likely to be interviewed by auditors to show the auditor how the system that is being examined actually works, and to restrict everything they say to answering the specific question actually asked by the auditor, rather than moving on to explain anything else that is not specifically, and tightly, on the subject of the question. This will demonstrate to the auditor that your people are tightly focused, and will also avoid the danger of someone talking so much that they lead the auditor to examine an aspect of your ISMS that doesn't need external examination.
5 Critically, ensure that management are fully involved in the certification audit. If necessary, rehearse with senior management the type of questions that they will be asked and the types of answers that they will be expected to give. While senior management should be perfectly capable of handling the audit (as they will

have been involved in and fully committed to the ISMS project from the outset), they may not be fully aware of how best to demonstrate this commitment to an external auditor. Done well, senior management's performance on the day can make a substantial contribution to certification success.

6 Be prepared to argue – constructively and calmly, but if there are issues on which you feel that an auditor has misunderstood your ISMS, or some aspect of it, or has misinterpreted the Standard, and is, as a result, considering recording a non-conformity (either major or minor), you should set out, calmly and firmly, why you believe that you are in the right. Auditors will respond negatively to any attempt to brow beat or belittle them; they will (usually) respond positively to any constructive attempt to help them achieve a better outcome. The greater their conviction that you are committed to the long-term effectiveness of your ISMS, the more prepared they will be to give you the benefit of any doubt on any marginal decisions.

Remember that, in a horse race, the difference between the horse that comes first and the one that comes second, doesn't need to be more than a nose, but the difference in prize money is substantial. In any certification project, it is always worth ensuring that you do everything as well as possible, because every little bit contributes to a successful outcome.

# ITG RESOURCES

IT Governance Ltd sources, creates and delivers products and services to meet the real-world, evolving IT governance needs of today's organisations, directors, managers and practitioners.

The ITG website (*www.itgovernance.co.uk*) is the international one-stop-shop for corporate and IT governance information, advice, guidance, books, tools, training and consultancy.

*www.itgovernance.co.uk/infosec.aspx* is the information page on our website for information security resources.

## Other Websites

Books and tools published by IT Governance Publishing (ITGP) are available from all business booksellers and are also immediately available from the following websites:

*www.itgovernance.eu* is our euro-denominated website which ships from Benelux and has a growing range of books in European languages other than English.

*www.itgovernanceusa.com* is a US$-based website that delivers the full range of IT Governance products to North America, and ships from within the continental US.

*www.itgovernance.in* provides a selected range of ITGP products specifically for customers in the Indian sub-continent.

*www.itgovernance.asia* delivers the full range of ITGP publications, serving countries across Asia Pacific. Shipping from Hong Kong, US dollars, Singapore dollars, Hong Kong dollars, New Zealand dollars and Thai baht are all accepted through the website.

**Toolkits**

ITG's unique range of toolkits includes the IT Governance Framework Toolkit, which contains all the tools and guidance that you will need in order to develop and implement an appropriate IT governance framework for your organisation.

For a free paper on how to use the proprietary Calder-Moir IT Governance Framework, and for a free trial version of the toolkit, see *www.itgovernance.co.uk/calder_moir.aspx*.

There is also a wide range of toolkits to simplify implementation of management systems, such as an ISO/IEC 27001 ISMS or an ISO/IEC 22301 BCMS, and these can all be viewed and purchased online at *www.itgovernance.co.uk*.

**Training Services**

IT Governance offers an extensive portfolio of training courses designed to educate information security, IT governance, risk management and compliance professionals. Our classroom and online training programmes will help you develop the skills required to deliver best practice and compliance to your organisation. They will also enhance your career by providing you with industry standard certifications and increased peer recognition. Our range of courses offer a structured learning path from Foundation to Advanced level in the key topics of information security, IT governance, business continuity and service management.

ISO/IEC 27001:2013 is the international management standard that helps businesses and organisations throughout the world develop a best-in-class Information Security Management System. Knowledge and experience in implementing and maintaining ISO27001 compliance are considered to be essential to building a successful career in information security. We have the world's first programme of certificated ISO27001 education with Foundation, Lead Implementer, Risk Management and Lead Auditor training courses. Each course is designed to provide

delegates with relevant knowledge and skills and an industry-recognised qualification awarded by the International Board for IT Governance Qualifications (IBITGQ).

Full details of all IT Governance training courses can be found at *www.itgovernance.co.uk/training.aspx*.

**Professional Services and Consultancy**

Your mission to plug critical security gaps will be greatly assisted by IT Governance consultants, who have advised hundreds of information security managers in the adoption of ISO27001 Information Security Management Systems (ISMS).

The organisation's assets, security and data systems, not to mention its reputation, are all in your hands. A major security breach could spell disaster. Timely advice and support from IT governance experts in tackling any, or all, of the Nine Steps to Success will enable you to identify the threats, assess risks and put in place the necessary controls before there's an incident.

At IT Governance, we understand that information, information security and information technology are always business issues, and not just IT ones. Our consultancy services assist you in managing information security strategies in harmony with business goals, conveying the right messages to your colleagues to support decision-making.

For more information about IT Governance Consultancy, see: *www.itgovernance.co.uk/consulting.aspx*.

**Publishing Services**

IT Governance Publishing (ITGP) is the world's leading IT-GRC publishing imprint that is wholly owned by IT Governance Ltd.

With books and tools covering all IT governance, risk and compliance frameworks, we are the publisher of choice for authors and distributors alike, producing unique and practical

publications of the highest quality, in the latest formats available, which readers will find invaluable.

*www.itgovernancepublishing.co.uk* is the website dedicated to ITGP enabling both current and future authors, distributors, readers and other interested parties, to have easier access to more information. This allows ITGP website visitors to keep up to date with the latest publications and news.

**Newsletter**

IT governance is one of the hottest topics in business today, not least because it is also the fastest moving.

You can stay up to date with the latest developments across the whole spectrum of IT governance subject matter, including; risk management, information security, ITIL and IT service management, project governance, compliance and so much more, by subscribing to ITG's core publications and topic alert emails.

Simply visit our subscription centre and select your preferences: *www.itgovernance.co.uk/newsletter.aspx*.