A Guide to Implementing the ISO/IEC 27001 Standard

Contents

1 INTRODUCTION 3

1.1 THE ISO/IEC 27001 STANDARD 3
1.2 THE CERTIKIT ISO/IEC 27001 TOOLKIT 6
1.3 IF YOU'RE A CLOUD SERVICE PROVIDER (CSP) 8
1.4 WHERE TO START 8
1.5 A SUGGESTED PROJECT PLAN 10
1.6 HOW THIS GUIDE IS STRUCTURED 12

2 IMPLEMENTING THE ISO/IEC 27001 STANDARD 13

2.1 SECTION 0 – INTRODUCTION 13
2.2 SECTION 1 – SCOPE 13
2.3 SECTION 2 – NORMATIVE REFERENCES 13
2.4 SECTION 3 – TERMS AND DEFINITIONS 13
2.5 SECTION 4 – CONTEXT OF THE ORGANIZATION 14
2.6 SECTION 5 - LEADERSHIP 15
2.6.1 Leadership and commitment 15
2.6.2 Policy 16
2.6.3 Organizational roles, responsibilities and authorities 16
2.7 SECTION 6 - PLANNING 16
2.7.1 Actions to address risks and opportunities 17
2.7.2 Information security objectives and planning to achieve them 19
2.8 SECTION 7 – SUPPORT 19
2.8.1 Resources 19
2.8.2 Competence 20
2.8.3 Awareness 20
2.8.4 Communication 20
2.8.5 Documented information 20
2.9 SECTION 8 - OPERATION 20
2.10 SECTION 9 – PERFORMANCE EVALUATION 21
2.10.1 Monitoring, measurement, analysis and evaluation 21
2.10.2 Internal Audit 22
2.10.3 Management review 22
2.11 SECTION 10 - IMPROVEMENT 23
2.11.1 Nonconformity and corrective action 23
2.11.2 Continual improvement 23

3 THE ANNEX A CONTROLS 24

3.1 A.5 INFORMATION SECURITY POLICIES 24
3.2 A.6 ORGANIZATION OF INFORMATION SECURITY 25
3.3 A.7 HUMAN RESOURCE SECURITY 26
3.4 A.8 ASSET MANAGEMENT 26
3.5 A.9 ACCESS CONTROL 28
3.6 A.10 CRYPTOGRAPHY 28
3.7 A.11 PHYSICAL AND ENVIRONMENTAL SECURITY 29
3.8 A.12 OPERATIONS SECURITY 29
3.9 A.13 COMMUNICATIONS SECURITY 30
3.10 A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE 31
3.11 A.15 SUPPLIER RELATIONSHIPS 31
3.12 A.16 INFORMATION SECURITY INCIDENT MANAGEMENT 32
3.13 A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 32
3.14 A.18 COMPLIANCE 33

4 ADVICE FOR THE AUDIT 34

4.1 CHOOSING AN AUDITOR 34
4.2 ARE WE READY FOR THE AUDIT? 37

4.3 PREPARING FOR AUDIT DAY 38
4.4 AT THE AUDIT 38
4.5 AFTER THE AUDIT 39
5 CONCLUSION 41

List of Figures

FIGURE 1 - OVERALL ISMS IMPLEMENTATION ORDER 11

1 Introduction

This concise guide takes you through the process of implementing the ISO/IEC 27001 international standard for information security. It provides a recommended route to certification against the standard starting from a position where very little is in place. Of course, every organization is different and there are many valid ways to embed the disciplines of information security. The best way for you may well depend upon a number of factors, including:

- The size of your organization
- The country or countries in which you operate
- The culture your organization has adopted
- The industry you operate within
- The resources you have at your disposal
- Your legal, regulatory and contractual environment

So view this guide simply as a pointer to where you could start and a broad indication of the order you could do things in. There is no single "right way" to implement information security; the important thing is that you end up with an Information Security Management System (ISMS) that is relevant and appropriate for your specific organization's needs.

Good luck!

1.1 The ISO/IEC 27001 standard

The ISO/IEC 27001 international standard for "Information technology — Security techniques — Information security management systems — Requirements" was originally published by the ISO and IEC in 2005 and is based upon the earlier British standard BS7799. Revised in 2013, ISO/IEC 27001 specifies the requirements that your ISMS will need to meet in order for your organization to become certified to the standard. The requirements in ISO/IEC 27001 are supplemented by guidance contained in ISO/IEC 27002 which was also revised in 2013. ISO/IEC 27002 is well worth reading as it fills in some of the gaps in understanding how the requirements in ISO/IEC 27001 should be met and gives more clues about what the auditor may be looking for.

There are a number of other documents published within the ISO/IEC 27000 series and many of them provide useful supporting information for organizations going for ISO/IEC 27001 certification (or simply using it for guidance). Some of the commonly-referenced ones are:

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27017 – Information security for cloud services

- ISO/IEC 27018 – Protecting Personally Identifiable Information in the cloud
- ISO/IEC 27032 — Guidelines for cybersecurity
- ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security
- ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security
- ISO/IEC 27035 — Information security incident management
- ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

It's worth pointing out that, although useful, none of these are required reading for ISO/IEC 27001 so if you are limited in time and budget, ISO/IEC 27002 is still your best bet.

There's no obligation to go for certification to ISO/IEC 27001 and many organizations choose to simply use the standard as a set of good practice principles to guide them along the way to managing their information security risks.

One subject worth mentioning is that of something the ISO calls "Annex SL". This is a very obscure name for a concept that represents a big change in ISO management system standards and ISO/IEC 27001 is an early adopter of this concept. There are a number of ISO standards that involve operating a "management system" to address the specific subject of the standard. Some of the main examples are:

ISO 9001	-	Quality management
ISO 14001	-	Environmental management
ISO 22301	-	Business continuity management
ISO/IEC 20000	-	IT service management

Traditionally, all of these standards have had a slightly different way of implementing and running a management system and the wording of the standards has varied sometimes quite significantly. This is ok until an organization decides to try to run a single management system across multiple standards, for example ISO9001 and ISO/IEC 27001. Then it becomes difficult for the organization to marry up differing ways of doing the same thing and it makes the auditors' job harder (and longer and more expensive) too.

So, to get around this problem of "multiple management systems" the ISO decided to standardise the wording of the management system parts of the standards. They produced a long document with numerous appendices, one of which was "Annex SL" containing a first draft of the standard wording. Over time the ISO is now phasing in this common "Annex SL" wording (also sometimes referred to as the "High Level Structure") and all new standards or new versions of existing standards will have it. ISO/IEC 27001 is one of the first to adopt this new layout and so may be called one of the first "Annex SL" standards. ISO has made good progress in phasing Annex SL in and a

number of standards, including ISO 22301 (business continuity) ISO 9001 (quality management systems) and ISO 14001 (environmental management systems) now have it.

So the good news for an organization implementing a ISMS based on ISO/IEC 27001 is that they will by default be putting in place an "Annex SL" management system. This will make it much easier for them to implement other standards such as ISO 9001 at a later date.

The ISO/IEC 27001 standard consists of a number of major headings which will be common across other standards (because they are the "Annex SL" headings) which are:

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Sections 0 to 3 don't contain any requirements and so an organization wouldn't be audited against those. They are worth a read however as they provide some useful background to what the standard is about and how it should be interpreted.

Sections 4 to 10 set out the requirements of the standard. Requirements are often referred to as the "shalls" of the standard because that is the word usually used by ISO to show that what is being stated is compulsory if an organization is to be compliant. So the (internal and external) auditing process is basically an exercise to check whether all of the requirements are being met by the organization. Requirements are not optional and, if they are not being met, then a "nonconformity" will be raised by the auditor and the organization will need to address it to gain or keep their certification to the standard (see the section on auditing later in this guide).

In order to show that the requirements are being met the auditor will need to see some evidence. This can take many forms and until recently was defined as a combination of "documents" (evidence of intention such as policies, processes and procedures) and "records" (evidence that something has been done). In the new version of the standard the term "documented information" is generally used instead to cover anything that is recorded (the official ISO definition is "information required to be controlled and maintained by an organization and the medium on which it is contained"). But the point is you need to have something to show the auditor.

This is often a major culture change in many organizations. Just doing something is no longer enough; you must be able to prove that you did something. This means keeping records in areas you maybe don't keep records at the moment, a good example often being meeting minutes. Meetings happen and things are discussed and decisions are made but the auditor won't just accept your

word for it. The auditor will want to see the minutes. Other examples could be training records – who was trained to do what and when? Information security vulnerability tests – what was tested, by whom, when and what was the outcome?

If all of this sounds rather onerous, then it's true, it can mean more work at least in the short term. But doing information security according to the ISO/IEC 27001 standard is about doing it right. You will be taking advantage of the knowledge of a wide variety of experienced people who have come together to define the best way to create a ISMS that works; people from all over the world in a wide variety of industries and organizations large and small.

From our experience what often happens during the process of implementing an international standard such as ISO/IEC 27001 is that initially you will put things in place because the standard says you should. Some of the requirements may seem unnecessary or over the top. But gradually you will start to see why they are included and the difference it makes to your organization. After a period of time you will begin to implement procedures and methods that go further than the requirements of the standard because you can see that they would be useful and will provide better protection for your organization. You'll start to see that it's about becoming more proactive in everything you do and in the long term this reduces the amount of reactive activities necessary. In simple terms, you'll start to "get it" (but be patient, it can take a while!).

But in the meantime, you'll need to create some of that "documented information". And that's where the CertiKit ISO/IEC 27001 Toolkit comes in….

1.2 The CertiKit ISO/IEC 27001 Toolkit

When looking at information security the emphasis is usually on risk assessment and the maintenance of controls to protect against risk. And it's right that this should be the main focus; it is, after all, the main deliverable of the whole information security idea.

In a perfect world we would just assess our risks, based on our intimate knowledge of the business and the threats to it and nothing would ever change. The controls would be appropriate and effective at all times, never need improving and everyone would know how to use them.

But we live in a far from perfect world where things can and do change on a regular basis, we don't know everything about the business, risks change, people come and go from the organization and our definition of what's important moves all the time.

So the ISO/IEC 27001 standard proposes that we don't just need a plan; we need an *Information Security Management System* or ISMS. The function of the ISMS is to wrap itself around the risk assessment and controls and ensure (among other things) that:

1. Everyone understands what we're trying to achieve (*Objectives*)
2. The risk assessment is based on the right information about the business (*Business context*)
3. We have a good idea of what the current main threats are (*Risk management*)

4. Everybody knows about the controls (including policies and procedures) and how to use them (*Awareness and training*)
5. We update the risk assessment when things change around it (*Management review*)
6. The level of protection in place gets better over time (*Continual improvement*)

The CertiKit ISO/IEC 27001 Toolkit (referred to within this document simply as the "Toolkit") provides not only the plan, but also a large part of the ISMS that supports it. So within your Toolkit you will have an array of useful documents which provide a starting point for all of the different areas of the standard. The documents are in Microsoft Office 2010® (or above) format and consist of Word documents, Excel workbooks, PowerPoint presentations, Visio diagrams and Project plans.

Each document is located within a folder structure that maps onto the various sections of the standard and is placed under the section that is most relevant to its content. Some documents are relevant to multiple sections of the standard and are placed in the one of greatest relevance.

A document reference naming convention is used throughout the Toolkit which is described in an *Information Security Management System Documentation Log*. This includes a reference to the section number of the ISO/IEC 27001 standard to which the document refers. The standard doesn't require that you use this specific naming convention so feel free to change it if you need to.

The documents themselves have a common layout and look and feel and adopt the same conventions for attributes such as page widths, fonts, headings, version information, headers and footers. Custom fields are used for the common items of information that need to be tailored such as [Organization Name] and these are easily changed in each document.

Every document starts with an "Implementation Guidance" section which describes its purpose, the specific areas of the ISO/IEC 27001 standard it is relevant to, general guidance about completing and reviewing it and some legal wording about licensing etc. Once read, this section, together with the CertiKit cover page, may be removed from the final version of the document.

The layout and headings of each document have been designed to guide you carefully towards meeting the requirements of the standard and example content has been provided to illustrate the type of information that should be given in the relevant place. This content is based upon an understanding of what a "typical" organization might want to say but it is very likely that your organization will vary from this profile in many ways so you will need to think carefully about what content to keep and what to change. The key to using the Toolkit successfully is to review and update each document in the context of your specific organization. Don't accept the contents without reading them and thinking about whether they meet your needs – does the document say what you want it to say, or do you need to change various aspects to make it match the way you do things? This is particularly relevant for policies and procedures where there is no "right" answer. The function of the document content is help you to assess what's right for you so use due care when considering it. Where the content is very likely to need to be amended we have highlighted these sections but please be aware that other non-highlighted sections may also make sense for you to update for your organization.

1.3 If You're a Cloud Service Provider (CSP)

If your organization is in the business of providing cloud services to your customers then two of the codes of practice within the list in section 1.1 above are particularly relevant to you. They are:

- ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

There is an increasing trend, led by the big CSPs, to declare conformance to one or both of these codes of practice in addition to their certification to the ISO/IEC 27001 standard.

The ISO/IEC 27001 standard and the ISO/IEC 27002 code of practice are fairly vague when it comes to the specifics of cloud services so ISO/IEC 27017 has been produced to plug that gap. The layout of the code of practice mirrors that of Annex A of ISO/IEC 27001 (and therefore ISO/IEC 27002) but goes into more detail about thirty-seven of the Annex A controls, with an extra seven added for good measure in areas such as virtual machine configuration and customer environment separation. Both the customer and supplier perspective are given, implying that the security of the cloud is very much a two-way deal.

With the EU General Data Protection Regulation (GDPR) soon coming into force and debate over the EU-US Privacy Shield, Privacy is a hot topic and the intention of ISO/IEC 27018 is to help organizations protect Personally Identifiable Information (PII) more effectively. As with ISO/IEC 27017, this standard builds on ISO/IEC 27001/2 but also introduces an extended control set for PII protection, covering areas such as consent and choice, data minimization and privacy compliance.

Because the use of these codes of practice is becoming more common and a significant number of CertiKit's customers are CSPs, we have addressed many of the additional requirements in ISO/IEC 27017 and 18 within the toolkit. The intention is that these sections are clearly marked where they only apply to CSPs so that for our non-CSP customers it shouldn't be confusing.

To sum up, for ISO/IEC 27001 certification, the guidance in these two codes of practice is not mandatory and as a CSP you can still become certified to ISO/IEC 27001 without implementing the additional controls they specify.

1.4 Where to start

Relevant Toolkit documents

- *CERTIKIT – ISO27001 In Simple English*
- *ISO-IEC 27001 Gap Assessment*
- *ISO-IEC 27001 Gap Assessment and Conformity Action Planning Tool*
- *ISO-IEC 27001 Assessment Evidence*

- *ISO-IEC 27001 Benefits Presentation*

Before embarking on a project to achieve conformity (and possibly certification) to the ISO/IEC 27001 standard it is very important to secure the commitment of top management to the idea. This is probably the single most significant factor in whether such a project (and the ongoing operation of the ISMS afterwards) will be successful. Indeed, "Leadership" has its own section within the standard and without it there is a danger that the ISMS will not be taken seriously by the rest of the organization and the resources necessary to make it work may not be available. In order to help your management decipher the meaning of the standard we have provided a Simple English translation of the requirements which aims to explain clearly each point without using "ISO-speak".

The first questions top management are likely to ask about a proposal to become certified to the ISO/IEC 27001 standard are probably:

- What are the benefits – why should we do it?
- How much will it cost?
- How long will it take?

In order to help answer these questions the CertiKit ISO/IEC 27001 Toolkit provides a number of resources.

The *ISO27001 Gap Assessment* is an Excel workbook that breaks down the sections of the ISO/IEC 27001 standard and provides a way of quantifying to what extent your organization currently meets the requirements contained within them. By performing this gap assessment you will gain a better appreciation of how much work may be involved in getting to a point where a certification audit is possible.

The optional *ISO27001 Gap Assessment and Conformity Action Planning Tool* (available at additional cost) goes several steps further by breaking down the text of the ISO27001 standard itself into individual requirements and providing a more detailed analysis of your conformance. It can also be used to allocate actions against individual requirements.

The key to making this gap assessment as accurate as possible is to get the right people involved so that you have a full understanding of what is already in place. The *ISO27001 Gap Assessment* will provide hard figures on how compliant you currently are by area of the standard and will even show you the position on bar charts to share with top management.

It's a good idea to repeat the exercise on a regular basis during your implementation project in order to assess your level of progress from the original starting point.

Note to Cloud Service Providers: we have also included a tab in the gap assessment to cover the ISO27017 and ISO27108 codes of practice (see section 1.3 above) so that, if you choose to, you can also see how close you are to conforming with these standards.

The accompanying workbook *Assessment Evidence* shows you how the various documents in the Toolkit map onto the requirements and what other evidence may be appropriate to show conformity. This may help when deciding whether a requirement is met or not.

Having gained an accurate view of where you are against the standard at the moment, you are then armed with the relevant information to assess how much effort and time will be required to achieve certification. This may be used as part of a presentation to top management about the proposal and a template *ISO/IEC 27001 Benefits Presentation* is provided in the Toolkit for this purpose. Note that budgetary proposals should include the costs of running the ISMS on an ongoing basis as well as the costs of putting it in place.

As part of your business case you may also need to obtain costs from one or more external auditing bodies for a Stage One and Stage Two review and ongoing surveillance audits (see later section about external auditing).

1.5 A suggested project plan

Relevant Toolkit documents

- *ISO-IEC 27001 Project Plan*
- *Information Security Management System Project Initiation Document (PID)*
- *ISO-IEC 27001 Progress Report*

Having secured top management commitment, you will now need to plan the implementation of your ISMS. Even if you're not using a formal project management method such as PRINCE2® we would still recommend that you do the bare essentials of defining, planning and tracking the implementation effort as a specific project.

We have provided a template Project Initiation Document (or PID) which prompts you to define what you're trying to achieve, who is involved, timescales, budget, progress reporting etc. so that everyone is clear from the outset about the scope and management of the project. This is also useful towards the end of the project when you come to review whether the project was a success.

Having written the PID, try to ensure it is formally signed off by top management and that copies of it are made available to everyone involved in the project so that a common understanding exists in all areas.

The CertiKit ISO/IEC 27001 Toolkit provides a Microsoft Project® plan as a starting point for your project (reproduced in Excel for non-Project users). This is fairly high level as the detail will be specific to your organization but it gives a good indication as to the rough order that the project should be approached in.

It's fair to say that in general if you implement your ISMS in the order of the ISO/IEC 27001 standard from section 4 to section 10 you won't go far wrong. This isn't necessarily true of some of the other

management system standards we have mentioned such as ISO/IEC 20000 but for ISO/IEC 27001, because it includes much of the information security content within a separate Annex A, it actually flows quite well.

The main steps along the way to certification are described in more detail later in this guide and there are some parts that need to be done in a certain order otherwise the right information won't be available in later steps. An example is that you need to complete your risk assessment before completing your Statement of Applicability because otherwise you won't have enough information to assess whether each control applies to your organization.

A simple twelve-step sequence for the route to certification is shown in figure 1 below. As suggested, this effectively steps through the standard in order although it starts with the foundation for the project (and for the ongoing ISMS) which is obtaining management commitment.

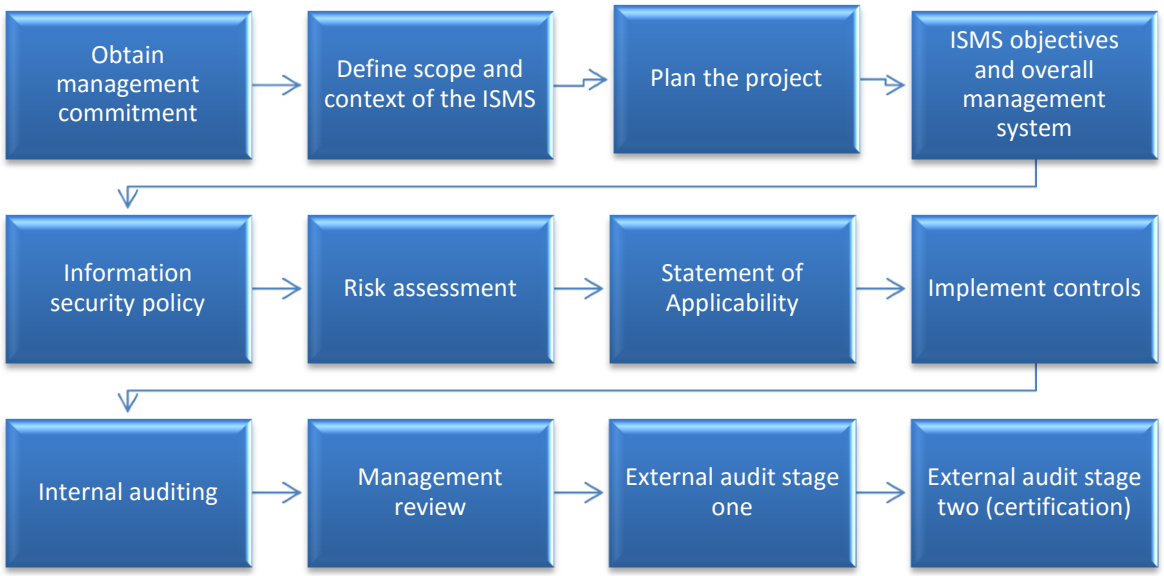

Figure 1 - Overall ISMS implementation order

Once a project manager has been appointed and the project planned and started, it's a good idea to keep an eye on the gap assessment you carried out earlier and update it as you continue your journey towards certification. This updated measurement of your closeness to complete conformity with the standard can be included as part of your regular progress reports and the CertiKit ISO/IEC 27001 Toolkit includes a template for these.

The timing of when to go for certification really depends upon your degree of urgency (for example you may need evidence of certification for a commercial bid or tender) and how ready you believe the organization to be. Certainly you will need to be able to show that all areas of the ISMS have been subject to internal audit before asking your external auditing body to carry out the stage two (certification) assessment. But you don't need to wait until you're "perfect", particularly as the

certification audit will almost certainly throw up things you hadn't thought of or hadn't previously regarded as important.

1.6 How this guide is structured

The remainder of this guide will take you through the sections of the ISO/IEC 27001 standard one by one, explaining what you may need to do in each area and showing how the various items in the CertiKit ISO/IEC 27001 Toolkit will help you to meet the requirements quickly and effectively.

As we've said earlier, regard this guide as helpful advice rather than as a detailed set of instructions to be followed without thought; every organization is different and the idea of an ISMS is that it moulds itself over time to fit your specific needs and priorities.

We also appreciate that you may be limited for time and so we have kept the guidance short and to the point, covering only what you need to know to achieve conformity and hopefully certification. There are many great books available on the subject of information security and we recommend that, if you have time, you invest in a few and supplement your knowledge as much as possible.

2 Implementing the ISO/IEC 27001 Standard

2.1 Section 0 – Introduction

The introduction to the standard is worth reading, if only once. It gives a good summary of what the ISO sees as the key components of an ISMS; this is relevant and important when understanding where the auditor is coming from in discussing what might be called the "spirit" of the ISMS. The detail in other sections of the standard should be seen in the context of these overall principles and it's important not to lose sight of that when all attention is focussed on the exact wording of a requirement.

There are no requirements to be met in this section.

2.2 Section 1 – Scope

This section refers to the scope of the standard rather than the scope of your ISMS. It explains the fact that the standard is a "one size fits all" document which is intended to apply across business sectors, countries and organization sizes and can be used for a variety of purposes.

There are no requirements to be met in this section.

2.3 Section 2 – Normative references

Some standards are supported by other documents which provide further information and are very useful if not essential in using the standard itself. For ISO/IEC 27001 the one quoted here is ISO/IEC 27000 which sets out the overview and vocabulary for an ISMS.

There are no requirements to be met in this section.

2.4 Section 3 – Terms and definitions

Unlike many other standards, ISO/IEC 27001 doesn't list any definitions at all, simply referring the reader to ISO/IEC 27000. If you feel you need to know the exact definitions of some of the terms used in ISO/IEC 27001 then this is the place to look, although in many cases you may not feel much more enlightened after reading the definition.

There are no requirements to be met in this section.

2.5 Section 4 – Context of the organization

Relevant Toolkit documents

- *Information security Context, Requirements and Scope*

This section is about understanding as much as possible about the organization itself and the environment in which it operates. The key point about the ISMS is that it should be appropriate and relevant to the specifics of the business it is protecting. To ensure this, the people implementing and running the ISMS must be able to answer questions about what the organization does, where, how and who for (plus many others).

The ISMS will also be affected by the situation within the organization (internal issues) and outside the organization (external issues). Internal issues are factors such as the culture, management structure, locations, management style, financial performance, employee relations, level of training etc. that define the organization. External issues are those less under the organization's control such as the economic, social, political and legal environment that it must operate within. All of these issues (internal and external) will have bearing on the priorities, objectives, operation and maintenance of the ISMS. This is particularly relevant when we discuss the areas of risk assessment and control selection where a comprehensive knowledge of how the organization operates and what could affect it are essential.

The standard also requires that the way in which the ISMS fits in with the controls already in place within the organization such as corporate risk management, business strategies and policies is defined and that all interested parties are identified, together with their needs and expectations.

One of the items that should be defined and documented is the organization's risk appetite. This refers to the overall attitude to risk; is the organization risk-averse and therefore wants to minimize risk at every level? Or is the attitude that of high risk/high reward where not everything will work out well but enough will deliver results to keep the company going? Or is it somewhere in between?

This needs careful consideration and discussion with top management; unless the organization is obviously very conservative or obviously very "high stakes" the answer is probably somewhere around the middle. This factor is used later on when deciding what to do about risks identified during a risk assessment – to treat them or to accept them. Risk appetite can be defined at many levels within the organization and so may vary according to what is being risk assessed and also at what point in time, so a clear understanding is very helpful.

The context section is also the one where the scope of the ISMS is defined. Again, this needs careful consideration. If your organization is small it usually makes sense to place everything it does within the scope because often it can be more difficult to manage a limitation to the scope than to simply cover everything. As the organization grows in size so do the issues with scope. There are three main

areas in which the scope might be limited; organization structure (e.g. one division or group company but not others), location (e.g. the Rome office but not the San Diego one) and product/service (e.g. the outsourcing/hosting service but not the software development service). It is perfectly acceptable to start with a smaller scope for certification and then widen it out year by year as the ISMS matures and everyone becomes more familiar with what's involved. In fact if you need to achieve certification within a short timescale this may well be the best route. You must ensure however that your exclusions make sense and can be justified to the auditor.

One point to note is the difference between the scope of the ISMS and the scope of certification to the ISO/IEC 27001 standard; they don't have to be the same. You can (if it's useful to do so) have a fairly wide ISMS scope but only ask for certification to a part of it initially. As long as the part in question meets all the requirements of the standard then it should be acceptable.

The Toolkit provides a template document that prompts for most of the information described above and groups the documented information required for context, requirements and scope into one place. It is perfectly acceptable to split this content into more than one document if that works better for you.

2.6 Section 5 - Leadership

Relevant Toolkit documents

- *Information Security Management System Policy*
- *Information Security Roles, Responsibilities and Authorities*
- *Executive Support Letter*
- *Meeting Minutes Template*

2.6.1 Leadership and commitment

The leadership section of the standard is about showing that top management are serious about the ISMS and are right behind it. They may do this in a number of ways. The first is by demonstrating management commitment; partly this is by simply saying that they support the ISMS in meetings, in articles in internal and external magazines, in presentations to employees and interested parties etc. and partly by making sure the right resources and processes are in place to support the ISMS e.g. people, budget, management reviews, plans etc. Sometimes these kinds of activities can be difficult to evidence to an auditor so within the Toolkit we have provided a number of documents that may help in this, including an executive support letter and a template for relevant meetings to be minuted.

2.6.2 Policy

The second way for top management to show they are serious about the ISMS is to ensure that there are appropriate information security policies in place. These need to be signed off by top management and distributed to everyone that they might be relevant to. A template ISMS policy is provided in the Toolkit that addresses the areas of commitment required by the standard and further policy documents are provided under the relevant sections within Annex A.

Generally most organizations take one of two approaches to policy creation; they either go for a single, all-encompassing information security policy or they go for a more modular approach with individual policies used to address specific issues. Both approaches have pros and cons, often depending on the size of your organization and how much work in involved in getting policy changes approved. If your organization is relatively small then we would recommend having a single policy document which covers all areas; however you will still need to consider the audience for the policy – there is no point in having technical detail about server security in a document that is intended to be understood by users, so you may still end up with a user-focussed policy and a more technical corporate policy anyway. If your organization is larger you may be best with a hierarchical structure of policies with the main points being approved at board level and the details defined at a lower management level. This means that if the detail changes you don't need to wait for a slot on the board agenda to get them approved each time. There isn't a single right answer for information security policies in the context of the ISO/IEC 27001 standard; the main point is that whatever you do choose to state in your policy(ies) then you can show that it is being communicated, understood and followed within the organization.

2.6.3 Organizational roles, responsibilities and authorities

Lastly, top management need to make sure that everyone involved in the ISMS knows what their role(s) and associated responsibilities and authorities are. Again, a document is provided in the Toolkit as a starting point for this. Remember to ensure that information security is included in the day to day responsibilities of existing roles rather than trying to create a parallel organization structure just for information security; it needs to be business as usual not an add-on.

Remember also that demonstrating leadership is an ongoing process, not a one-off activity solely during implementation.

2.7 Section 6 - Planning

Relevant Toolkit documents

- *Information Security Objectives and Plan*
- *Risk Assessment and Treatment Process*

- *Asset-Based Risk Assessment Report*
- *Scenario-Based Risk Assessment Report*
- *Risk Treatment Plan*
- *Risk Assessment and Treatment Workbook*
- *Statement of Applicability*

2.7.1 Actions to address risks and opportunities

The general ethos of the ISO/IEC 27001 standard is to be proactive in managing information security and a central concept to this is risk assessment. This involves considering what could go wrong and then taking steps to do something about it in advance rather than waiting for it to happen. The standard points out that not everything that happens is necessarily negative and that there may be positive "opportunities" along the way too.

The whole idea of a risk-based approach is that the amount you spend on controls is appropriate to your level of risk and also takes account of how much risk you are prepared to live with. Risk is very much a spectrum as the wider debate on "privacy versus security" shows and your organization will need to take a considered approach to the level of controls it chooses to introduce and maintain to provide the "right" level of security. A risk assessment needs to be conducted to analyse and evaluate the impact and likelihood of various events occurring. This will give you the opportunity to do something about those risks that are both likely and have a significant impact i.e. to treat the risks.

There are many ways of analysing risk and the ISO/IEC 27001 standard mentions that another standard, ISO 31000, should be used as a framework for this. ISO31000 is worth a read and sets out how to establish an organization-wide framework for risk assessment, not just for information security purposes but for all potential risks to the business. But ISO31000 itself doesn't go into detail about *how* risks should be identified; there are yet two more standards that fill this gap - ISO31010 and ISO/IEC 27005. You may realise from this that risk assessment is a very big subject in itself and there are very many techniques available to use if you choose to; ISO/IEC 27001 doesn't dictate which one to use and our recommendation is that you keep it as simple as possible, depending on the size of your organization and how much time you have.

The previous version of the ISO/IEC 27001 standard (published in 2005) required that an organization take an "asset-based" approach to risk assessment. This involved focussing on the organization's information assets and then considering the threats to them and their vulnerabilities to those threats. The 2013 version of the standard removed the requirement to take this approach, although it remains a perfectly valid way to assess risk. In the Toolkit we have provided a choice of an asset-based approach and a simplified scenario-based approach; either is compatible with the standard and it is up to you to decide which one works best within your organization.

Both risk assessment processes are compatible with the ISO31000 standard. Effective risk identification can often be done by simply getting the right people with the relevant knowledge in to a room and asking them about what they worry about most with regard to their area of responsibility. This should give you a good starting point to assess the risks that they identify.

Consult other parties such as external consultants and authorities where appropriate to get as good a picture as possible.

The identified risks may be entered into the *Risk Assessment and Treatment Workbook* which helps you to assess the likelihood and impact of each risk, giving a risk score. The workbook uses a defined classification scheme to label each risk as high, medium or low risk, depending on its score. A template *Risk Assessment Report* is provided in the Toolkit to communicate the findings of the risk assessment to top management and so that they can sign it off.

Whether or not each risk needs to be treated depends upon the risk appetite you defined in section 4.1 of the ISO/IEC 27001 standard (Understanding of the organization and its context). For those risks that do need treatment there are three main options:

1. Modify – take some action to reduce the likelihood or impact of the risk
2. Avoid – stop performing the activity that gives rise to the risk
3. Share – get another party to assume all or part of the risk (e.g. insurance)

Each of these options will have some effect on either the likelihood or impact of the risk, or both. The *Risk Assessment and Treatment Workbook* allows you to define what effect you believe the treatment will have in order to decide whether it is sufficient.

Once the risks have been identified, assessed and evaluated, the risk treatment plan is created. Again the Toolkit has a template plan which may be used to obtain top management approval of the recommended risk treatments, some of which may involve spending money. Top management also need to agree to the levels of residual risk after the treatments have been implemented (i.e. the risks we're left with once we've done everything proposed).

At this point the standard requires that a specific document called the "Statement of Applicability" be prepared which shows which of the reference controls in Annex A have been adopted and which haven't. Each decision to adopt or not must be justified, ideally by reference to a specific risk you have found that needs to be treated. Some of the reference controls will only apply in certain circumstances so if these don't apply to your organization (or your ISMS scope) then it is acceptable to state that you are not implementing them. Examples might be that Control *A.6.2.2 Teleworking* may not apply if you have no teleworkers or Control *A.14.2.6 Secure development environment* may not be relevant if no software development takes place.

The key point to remember in treating risk is that it is a trade-off. Few organizations have limitless funds and so the money spent in treating risk needs to result in a larger benefit than the cost. There are many ways of performing this kind of "quantitative" analysis so that the potential loss from a risk can be expressed in financial terms. The methods used in the Toolkit are "qualitative" in that they simply categorize the risks; if your organization wishes to use more detailed quantitative methods to assess risk loss against cost of treatment then that is perfectly acceptable within the ISO/IEC 27001 standard.

2.7.2 Information security objectives and planning to achieve them

Within the planning section of the standard we need to set out what the ISMS is intended to achieve and how it will be done. With regard to the ISMS there are two main levels of objectives. The first is the high level objectives set out when defining the context of the ISMS. These tend to be quite broad and non-specific in order to describe why the ISMS is necessary in the first place and these objectives probably won't change much.

The second level of objectives is more action-oriented and will refer to a fixed timeframe. In the Toolkit we have provided an information security management plan for a financial year on the assumption that a one year planning horizon will be used, but this could be a two or three year plan if that makes sense in your organization. The plan sets out specific objectives, including how success will be measured, the timeframe and who is responsible for getting it done. You may choose to create a Gantt chart in MS Project or similar to support this.

2.8 Section 7 – Support

Relevant Toolkit documents

- *Information Security Competence Development Procedure*
- *Information Security Communication Programme*
- *Procedure for the Control of Documented Information*
- *ISMS Documentation Log*
- *Information Security Competence Development Report*
- *Awareness Training*
- *Competence Development Questionnaire*

Covering resources, competence, awareness, communication and documented information, this section describes some of the background areas that need to be in place for the ISMS to function properly.

2.8.1 Resources

The standard simply requires that adequate resources are provided for the ISMS to function effectively. This is really a test of the level of management commitment as described earlier.

2.8.2 Competence

The Toolkit provides a method of defining the competences needed, conducting a survey of the people involved in the implementation and running of the ISMS, collating the results and then reporting on those areas in which further training or knowledge needs to be gained. You will need to ensure that appropriate records of training are kept and are available to view by the auditor.

2.8.3 Awareness

A template information security awareness presentation is also provided. This may be delivered in various ways, including at specially-arranged events or at regular team meetings, depending on the timescale required and the opportunities available. Note that the focus of this is awareness rather than detailed training and that anyone with a more involved role to play in the ISMS may need more in depth training.

2.8.4 Communication

Specific procedures may be required relating to business as usual communication with internal and external parties on the subject of information security; these may be relevant to this section of the standard and a template document *Information Security Communication Programme* is provided in the Toolkit.

2.8.5 Documented information

Documented information required by the standard must be controlled which basically means keeping it secure, managing changes to it and ensuring that those that need it have access to it. A procedure that covers the requirements for document control is provided and you will need to decide where such documentation is to be held. In modern times this is usually electronically and could be on a shared network drive, an intranet, a full-blown document management system or any other arrangement that is appropriate to your organization.

2.9 Section 8 - Operation

Relevant Toolkit documents

- *Supplier Information Security Evaluation Process*

Interestingly, this section of the ISO/IEC 27001 standard is very short and basically repeats what has been stated in other sections. This is in contrast to other standards such as ISO22301 (business continuity) where the majority of the requirements are within the Operation section.

The Toolkit includes a process to evaluate suppliers within the organization's supply chain, particularly as part of the requirement to determine and control outsourced processes and this should be used in conjunction with the documents addressing Control *A.15 Supplier relationships* within Annex A.

2.10 Section 9 – Performance evaluation

Relevant Toolkit documents

- *Process for Monitoring, Measurement, Analysis and Evaluation*
- *Procedure for Internal Audits*
- *Internal Audit Plan*
- *Internal Audit Schedule*
- *Internal Audit Checklist*
- *Internal Audit Report*
- *Internal Audit Action Plan*
- *Procedure for Management Reviews*
- *Management Review Meeting Agenda*

The performance evaluation section of the standard is about how you determine whether the ISMS is doing what it is supposed to do.

2.10.1 Monitoring, measurement, analysis and evaluation

The ISO/IEC 27001 standard does not tell you what you should measure. It simply requires that you be precise about what it is you have decided to measure and that you do something about it if your measurements show some kind of problem. The auditor will expect you to have put some thought into the appropriate measurements to take, how they can be taken and how the results can be reasonably interpreted. The Toolkit provides a document entitled *Process for Monitoring, Measurement, Analysis and Evaluation* which includes suggestions for the types of measurements that might be suitable for a typical organization but you will need to look at these carefully before using them. It's a good idea to create a documented procedure for the collection and reporting of each measurement because if it is done differently each time then the results will not be helpful.

This is an area that can start relatively small and expand over time; our recommendation is that you select some basic measurements that are easy to collect and interpret and use those for a while.

After some time has passed it will probably become obvious that other specific measurements are needed to be able to assess whether things are going well so these can be added gradually. Be careful not to start with a wide range of possibly meaningless, hard to collect measurements that will simply slow everything down and give the ISMS a bad reputation before it has got going.

Having chosen your measurements you need to decide what does "good" look like; what numerical values would mean that performance is in line with expectations? Again, the definition of your objectives may need tweaking over time as you gain experience with taking the measurements and your ISMS moves from implementation mode into ongoing operation mode.

If you find that your objectives are not being met then an improvement may be required to bring the situation back into line; such improvements should be added to the *Nonconformity and Corrective Action Log* provided within the Toolkit and tracked through to completion.

2.10.2 Internal Audit

The standard requires that there is an internal auditing programme in place which audits all aspects of the ISMS within a reasonable period of time. If you embrace the idea of internal auditing as a useful early warning of any issues at external audit then you won't go far wrong. Internal audits should ensure that there are no surprises during the annual certification/surveillance audit which should allow everyone a higher degree of confidence in the ISMS.

In terms of where to start auditing, the standard suggests that you take into account the importance of the processes concerned, problem areas identified in previous audits and those parts of the ISMS where significant risks have been identified. Beyond that, there is no particular order in which internal audits need to happen. Auditors need to be suitably qualified either through experience or training (or both) and must be impartial i.e. they are not involved in the setting up or running of the ISMS.

The Toolkit has a number of documents to help with the internal auditing process, including a schedule, plan, procedure, checklist of questions, report and post-audit action plan. In general, all aspects of internal auditing need to be documented and an external auditor will almost always want to see the most recent internal audit report and track through any actions arising from it.

2.10.3 Management review

Management review is another key part of the ISMS which, if you get it right, will hold together everything else and make audits (internal and external) a relatively straightforward experience. The ISO/IEC 27001 standard is pretty specific about what these reviews should cover but it is less forthcoming about how often they should take place. This is one of those areas where you will need to try it and see what works for your organization; too often and it becomes an unacceptable administrative overhead; too infrequent and you risk losing control of your ISMS. The generally

accepted minimum frequency is probably once a year and in this case it would need to be a full review covering everything required by the standard. A more common approach is to split the management review into two parts; perhaps a quarterly review of the main areas with a more complete review on an annual basis. You may even decide that in the early days of the ISMS a monthly review is appropriate. There is no wrong answer, there's just a decision about how much control you feel you need to exercise at management level.

In all cases, every management review must be minuted and the resulting actions tracked through to completion.

2.11 Section 10 - Improvement

Relevant Toolkit documents

- *Procedure for the Management of Nonconformity*
- *Nonconformity and Corrective Action Log*

2.11.1 Nonconformity and corrective action

Despite the section heading of "Improvement", this section of the standard talks mostly about nonconformities and corrective actions. The ISO definition of a nonconformity is the rather general "non-fulfilment of a requirement" and since a requirement can be pretty much anything, it is best to bring any actions, requests, ideas etc. together in a single place and manage them from there. The Toolkit provides the *Nonconformity and Corrective Action Log* for this purpose. A procedure is also provided which explains how items are added to the list, evaluated and then tracked through to completion.

2.11.2 Continual improvement

Continual improvement used to get a lot more attention in previous version of this and similar standards, but the requirements have now become considerably watered down, with only a general commitment needed to show conformity. The best place to evidence improvement is probably as part of management reviews where this is one of the standard agenda items – make sure your improvement actions are minuted.

3 The Annex A Controls

The reference controls within Annex A of the ISO/IEC 27001 standard form a significant part of the overall document and of the implementation effort involved. But it's easy to make the mistake of assuming that because these controls are listed in the standard that they have to be implemented to become certified. This is not necessarily the case.

The 114 controls within Annex A are effectively a menu to be chosen from when creating your risk treatment plan. Some of them may not be required because they address a risk you don't have. Similarly, you may decide to address a risk using a different control than the suggested one from Annex A; this is acceptable. However it may also be the case that you need to introduce *more* controls than those in Annex A if your level of risk in a particular area is very high.

The key is to adopt a considered, sensible approach based on what your risk assessment is telling you. As long as you feel you can justify your actions to an auditor, then varying the controls from those in Annex A is not a barrier to certification.

Having said this, the controls within Annex A are very sensible measures which, taken together, allow many different areas of risk to be addressed in a comprehensive way so think hard before you decide to do anything different; your default position should be that you will implement the Annex A control.

Remember that ISO/IEC 27002 provides more detail about each of the controls; the advice given below is a summary of the main points about each control area and how the documents within the Toolkit will help you to implement the set of controls.

3.1 A.5 Information security policies

Relevant Toolkit documents

- *Information Security Summary Card*
- *Internet Acceptable Use Policy*
- *Cloud Computing Policy*
- *Cloud Service Specifications (CSPs only)*

Policies are an important part of the ISMS and are either required or recommended in many places within the standard. Such policies set out the general approach that the organization is taking to a subject and usually include the "dos and don'ts" for that area. They don't have to be lengthy; in fact many would recommend that they actually be as short as possible because unless they are read by those they are aimed at they will have little effect.

In most cases, the ISO/IEC 27001 standard doesn't dictate what should be said in a particular policy. However it does emphasise that a policy should be approved by top management and communicated to those it is intended to apply to, so it may be useful to either get employees to sign a copy to say they have read it or keep records of attendees at briefing sessions (or both). It is also important that the contents of the policy are taken seriously and an auditor will often raise a nonconformity if a policy states that something should be done and it isn't. So measures to implement all of the contents of your policies should either already be in place or on your improvement plan to do in the near future.

3.2 A.6 Organization of information security

Relevant Toolkit documents

- *Segregation of Duties Guidelines*
- *Authorities and Specialist Group Contacts*
- *Information Security Guidelines for Project Management*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Segregation of Duties Worksheet*

These seven controls cover a wide range of areas, including some duplication of requirements in the main body of the standard (e.g. roles and responsibilities). In many more traditional areas such as finance, segregation of duties will already be in place but be careful where new processes are implemented. Contact with authorities and special interest groups is generally easy nowadays with the growth of online facilities such as discussion forums but it may be better to focus on a few important and relevant groups rather than spreading your time too thinly.

If your organization doesn't have a formal project management approach then this may be a good time to start to define one, even if it simply includes the basics. It would help to get your information classification scheme in place first (see *A.8.2 Information classification*) as this will provide a framework to use within your projects.

Mobile devices are obviously an area of increasing importance as they become more powerful and widespread so it's worth spending some time in this area to ensure your policy is as appropriate as possible. The difference between mobile working and teleworking is becoming increasingly blurred so it may make sense to merge these policies if that works for you.

3.3 A.7 Human resource security

Relevant Toolkit documents

- *Employee Screening Procedure*
- *Guidelines for Inclusion in Employment Contracts*
- *Employee Disciplinary Procedure*
- *Employee Screening Checklist*
- *New Starter Checklist*
- *Employee Termination and Change of Employment Checklist*
- *Personal Commitment Statement*
- *Leavers Letter*

You will need to work with your Human Resources department to implement most of the controls in this section. In most cases this will involve reviewing the existing procedures and documents to see if they cover information security sufficiently. Be careful that you will need to check that any changes you make comply with the laws of the country in which they will be implemented as employment law can be a bit of a minefield.

The human factor is often cited as being the single most important issue in promoting effective information security; this section is intended to ensure that you recruit the right people, they know their responsibilities and action can be taken if they don't fulfil them adequately.

3.4 A.8 Asset management

Relevant Toolkit documents

- *Information Asset Inventory*
- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Asset Handling Procedure*
- *Procedure for the Management of Removable Media*
- *Physical Media Transfer Procedure*

A good asset list is fundamental to the operation of the ISMS so this is another area where your time will be well spent. It's important to understand exactly what it is you are trying to protect and what value these assets have to your organization, so make sure you involve the right people in assessing them.

Similarly, information classification is central to the success of many other areas so put some thought into this; aim for a scheme that is practical, understandable and usable by everyone rather than trying to overcomplicate the situation. The ISO/IEC 27001 standard doesn't say much about information classification (although the ISO/IEC 27002 guidance publication has some useful tips) so the details of how you implement the control are pretty much left up to you. The first decision to make is how many levels of classification to have. It's tempting to over-complicate this in order to reflect the various nuances of your information, but our advice would be to resist this temptation and stick to the lowest number you can reasonably get away with. The trend amongst governments is in this direction, with the UK having recently reduced its classification levels from five to three (Official, Secret and Top Secret), so you'll be in good company. This doesn't include information that isn't classified at all, often referred to as "Public" and which doesn't need to be protected or labelled.

Choice of names for your classification levels are also up to you. Some of the most common choices are (listed from highest to lowest):

- Top secret
- Secret
- Confidential
- Restricted
- Protected
- Internal Use Only

Names chosen should be appropriate to your organization and a clear definition given of what they mean in practical terms.

Having decided what you're going to call your classification levels, how do you make it clear to everyone involved which information carries which level? Often organizations feel slightly overwhelmed with the thought that they have to suddenly label every single electronic and paper document they have, whilst working out what to do with data held in computer systems too.

The key here is to define an approach that addresses the important stuff first and puts a stake in the ground so that labelling starts from a specified point. Look to label the really confidential, high-value information first as this is likely to be a much smaller volume than the day-to-day less sensitive information. This requires you to have an accurate asset inventory (control 8.1.1 Inventory of assets) so that you know what you're dealing with. An approach that begins to label all new assets from a certain date will make you feel you are starting to get some control over the issue, whilst considering how to address the historical items. Information assets should have owners and they are the ones who should be looking at labelling so it's not all down to a single person or department to achieve it; spread the load as much as possible.

Grouping items with the same classification level will also help to make things clear without a huge administrative overhead. Maybe everything held in a particular room is confidential and locking the door and labelling it as such will be enough to meet the need. You may need to invest in a stamp for existing paper copies that need to be individually labelled, but obviously items that are printed in the future should be electronically labelled using headers, footers, watermarks etc.

There are software tools available to help you with this task. These can use metadata to reflect classification level and then prevent certain types of documents being used in particular ways according to a defined policy e.g. confidential documents should not be emailed outside the organization. In some cases a home-grown solution using existing facilities within office software etc. may work just as well.

Having classified and labelled our assets, we also need to make sure that they remain appropriately protected throughout their lives, particularly if they go beyond the organization's boundaries e.g. to another location via courier or to a third party via electronic transfer. This is really about understanding the ways in which your information assets are used and ensuring that procedures are in place to keep them secure. Again, starting with the highest level assets is usually a good idea. This is an area in which there have been many notorious public breaches to do with government departments with sensitive information such as names, addresses and tax information going missing, sometimes in unencrypted form.

So think about whether your information is saved onto other media, printed, transmitted, emailed or otherwise processed in a way that makes a procedure necessary.

Removable media is a common subject of attention from the auditor so try to ensure that everyone is aware of the policy and that items are not left lying around the office.

3.5 A.9 Access control

Relevant Toolkit documents

- *Access Control Policy*
- *User Access Management Process*

Most organizations will have access control in place so addressing these control requirements is mainly a case of tightening things up rather than starting from scratch. An access management audit is often a good starting point to identify users who have access they shouldn't and to highlight areas where existing procedures aren't working. A clear policy and revised procedures that are strictly followed will address most requirements, supplemented by a regular repeat of the access management audit/review.

3.6 A.10 Cryptography

Relevant Toolkit documents

- *Cryptographic Policy*

Although the standard only refers to policies for cryptography and key management, you will probably need to ensure that accurate procedures are developed and used for common cryptography-related tasks such as encrypting the hard disks of laptops. As the use of encryption grows, especially in a cloud environment, it will become harder to manage the variety of keys used and the consequences of losing a key can be severe so it is important to get this right.

3.7 A.11 Physical and environmental security

Relevant Toolkit documents

- *Physical Security Policy*
- *Physical Security Design Standards*
- *Procedure for Working in Secure Areas*
- *Data Centre Access Procedure*
- *Procedure for Taking Assets Offsite*
- *Equipment Maintenance Schedule*

This set of controls will involve more work the larger and more numerous the offices and other facilities you have. You may need to spend some money to upgrade the security precautions in place and ensure that the different types of area (e.g. delivery and loading areas) are well-defined. However a key part of this will be to ensure that all employees have an awareness of their responsibilities for physical security e.g. challenging unescorted strangers, closing windows.

In many organizations the adoption of a clear desk policy can be challenging and the cost of additional secure storage can add up. Remember however that the policy is likely to only apply to items of a certain security classification so publicly available information may still be sited on desks.

3.8 A.12 Operations security

Relevant Toolkit documents

- *Operating Procedure*
- *Change Management Process*
- *Capacity Plan*
- *Anti-Malware Policy*
- *Backup Policy*
- *Procedure for Monitoring the Use of IT Systems*

- *Software Policy*
- *Technical Vulnerability Management Policy*
- *Technical Vulnerability Assessment Procedure*
- *Information Systems Audit Plan*

This is another large section with many controls, some of which could potentially take significant effort to implement. For example change and capacity management are two areas which, to do properly in a large environment, could be major projects in themselves; our recommendation is to focus on the most critical aspects of your infrastructure and bring these under control first and document templates are provided to help with this.

It is likely that malware and backup controls are already in place as they are standard IT procedures and these may simply need revisiting to ensure they are comprehensive and accurate.

The management of event logs is made much easier using software tools and there are many available, including some open source ones. The key is to be able to detect any exception situations within the mass of log data and react to them appropriately.

Technical vulnerability management will in most cases mean patching and this may be sufficient to meet the control requirement, but it is always worth looking at running a vulnerability scanner on a regular basis to check your exposure.

3.9 A.13 Communications security

Relevant Toolkit documents

- *Network Security Policy*
- *Network Services Agreement*
- *Information Transfer Agreement*
- *Information Transfer Procedure*
- *Electronic Messaging Policy*
- *Schedule of Confidentiality Agreements*
- *Non-Disclosure Agreement*

A comprehensive network diagram is the best starting point in satisfying the control requirements in this section. This needs to cover not only internal networks but also links with external third parties and an appreciation of the data transferred via the networks will help to identify the need for encryption and transfer agreements to be in place.

3.10 A.14 System acquisition, development and maintenance

Relevant Toolkit documents

- *Requirements Specification*
- *Secure Development Policy*
- *Principles for Engineering Secure Systems*
- *Secure Development Environment Guidelines*
- *Acceptance Testing Checklist*

If your organization develops its own software then it is likely that all of these controls will apply. If it doesn't then the number of applicable controls will depend upon whether software development is outsourced or purely commercial off the shelf (COTS) software is used. Remember that even COTS software still needs to be tested in a secure way so test-related controls will still be needed.

Tender documents for new systems will need to show consideration of information security issues, including how data transmitted over the Internet will be protected e.g. using strong encryption.

For organizations in the software development business an auditor would expect a good degree of effort to be spent in developing code with as few vulnerabilities as possible, with changes tightly controlled and effective segregation of duties in place (e.g. developers cannot promote code to production).

3.11 A.15 Supplier relationships

Relevant Toolkit documents

- *Information Security Policy for Supplier Relationships*
- *Supplier Information Security Agreement*
- *Supplier Due Diligence Assessment Procedure*
- *Supplier Due Diligence Assessment*
- *Cloud Supplier Questionnaire*

A chain is only as strong as its weakest link and if you share sensitive information with your suppliers then the standard requires you to take adequate measures to ensure that they protect it as well as you do. This may be achieved via a combination of second party audits (see *Supplier Information Security Evaluation Process*), contractual agreements and strong access control over remote links to and from suppliers.

Much of this will depend on how important a customer you are to your suppliers; small organizations who are customers of large suppliers may have less influence over contractual terms and the security controls in place. This should be considered when deciding which supplier to choose in any particular situation.

3.12 A.16 Information security incident management

Relevant Toolkit documents

- *Information Security Event Assessment Procedure*
- *Information Security Incident Response Procedure*

It's easy to ignore the event management requirements of the standard and focus on incidents, but doing this risks falling foul of the auditor. In your information security environment you will most likely be bombarded with things that happen on a daily basis that may or may not be incidents and being able to work out the difference quickly will be key. Ensure you have a clear approach to assessing events to decide whether or not you've been breached as crying wolf too often will get you a bad reputation.

Information security incident management is becoming increasingly important as organizations realize that preventing all breaches is virtually impossible. If you have an existing IT incident management process (usually provided via an IT service or help desk) it may make sense to enhance this to cover information security incidents rather than have a separate process running side by side.

For major breaches with potentially significant consequences for the reputation of the organization the best approach is to be prepared and well drilled in your response. This situation has a lot in common with a business continuity event and should be managed in much the same way, with senior management involvement from the outset.

One of the main differences for information security incidents may be the need to preserve evidence for later investigation and possibly legal action or prosecution, particularly where there may have been fraud carried out by an insider.

3.13 A.17 Information security aspects of business continuity management

Relevant Toolkit documents

- *Business Continuity Incident Response Procedure*
- *Business Continuity Plan*
- *Business Continuity Exercising and Testing Schedule*

- *Business Continuity Test Plan*
- *Business Continuity Test Report*
- *Availability Management Policy*

The key point to make with regard to business continuity in the context of the ISO/IEC 27001 standard is that the control requirements in this section refer to the *information security* aspects of your BC plan, if you have one; there is no explicit requirement to have a BC plan as such (this is covered by a separate international standard, ISO 22301). The requirements are to ensure that, if a disruptive event occurs, your information remains protected as far as possible and that any actions you take as part of recovery do not circumvent the controls you have in place (or other compensating controls should be used).

3.14 A.18 Compliance

Relevant Toolkit documents

- *Legal, Regulatory and Contractual Requirements Procedure*
- *Legal, Regulatory and Contractual Requirements*
- *IP and Copyright Compliance Policy*
- *Records Retention and Protection Policy*
- *Privacy and Personal Data Protection Policy*

It is important that your organization has a full understanding of its responsibilities from a legal viewpoint, including protection of intellectual property, personally identifiable information and other forms of record. Depending on your industry there may also be other requirements specified by a regulator e.g. in the finance or health industries.

Legislation varies significantly by country so you will need to either take appropriate legal advice or conduct adequate research to establish which laws apply, and your responsibilities under them. You will also need to keep this understanding up to date as things change.

Lastly, information security reviews should be undertaken on a regular basis; some of these can be done as part of the internal audit and management review processes but technical compliance reviews of key systems may need to be performed as separate, discrete exercises which must be documented.

4 Advice for the Audit

4.1 Choosing an Auditor

If your organization wishes to become certified to the ISO/IEC 27001 standard, it will need to undergo a two stage process performed by a suitable external auditing body. Before this, you will need to select your auditing body and in most countries there are a variety of options. If you are already certified to a different international standard such as ISO 9001 then it usually makes sense to use the same auditing company for ISO/IEC 27001, as long as they can provide that service. Increasingly, multi-standard audits will become commonplace as the effects of the Annex SL revisions are felt (see section 1.1 The ISO/IEC 27001 standard).

There are many companies that offer certification audits and your choice will obviously depend upon a variety of factors including where in the world you are based. However, there are a few general things you need to be aware of before you sign up with any particular auditor.

Self-certification

The first is to emphasize the fact that ISO standards are not legal documents; the creation, maintenance and adoption of ISO standards is a voluntary exercise that is co-ordinated by the ISO. Yes, ISO owns the copyright and sells standards for cash both directly and through third parties, but rest assured that you won't be breaking any laws if you don't quite implement a standard in full. And the same goes for declaring compliance with ISO standards. You have a choice.

You could simply tell everyone you deal with that you meet the requirements of a particular ISO standard. That's it – no audit fees or uncomfortable visits from men in suits. Just say that you comply. The trouble with this is that if everyone did it, there would be no way of telling the difference between good organizations that really had done it properly and less conscientious ones that just paid the standard lip service. It only takes a few bad apples to spoil it for everybody. The people that matter to you (e.g. your customers or regulators) may simply not believe you.

Third party certification

So instead you may decide to get a third party to test your implementation of a standard and testify that you've done it properly. This is where Registered Certification Bodies (RCBs) come in. An RCB is a company that has the expertise and resources to check that you do indeed meet the requirements of the standard and is willing to tell others that you do. But hold on, how do your customers know that the RCB itself can be trusted to have done a good job of the audit?

What's needed is another organization that is trusted to check the auditors and make sure that they are doing a good job. But how do we know they can be trusted? And so it goes on. What we end up with is a chain of trust similar to the way that Public Key Infrastructure works. At this point we need to introduce you to a few important definitions:

Certification **-** this is what happens when you are audited against a standard and you (hopefully) end up with a certificate to put on the wall (as in "we are certified to ISO/IEC 27001").

RCB **-** a Registered Certification Body is basically an auditing company that has been accredited to carry out certification audits and issue a certificate to say you are compliant with a particular standard. Some operate in a single country and some in a lot of countries. This is what you, as an organization wanting to become certified, need to choose.

Accreditation - this is what the auditors go through to become an RCB and allow them to carry out certification audits.

Ok, now we've got those definitions out of the way we need to talk about who actually does the accrediting. There are basically two levels, international and national.

IAF

Based in Quebec, Canada, the International Accreditation Forum is the worldwide body that represents the highest level of trust concerning accreditation of RCBs. They have lots of strict rules that national accreditation bodies must agree to, embodied in a charter and a code of conduct. All of the national accreditation bodies are members of the IAF.

ANAB

As if there weren't enough acronyms in the world, here we have an acronym within an acronym. ANAB stands for the ANSI-ASQ National Accreditation Board. ANSI is the American National Standards Institute and deals with standards in the USA. ASQ is the American Society for Quality and although based in the USA, has a more international reach than ANSI. So put them together and you get ANAB which is the national accreditation body for the USA and therefore a member of the IAF.

UKAS

The United Kingdom Accreditation Service is the body in the United Kingdom that accredits RCBs. It is effectively the UK representative of the IAF.

JAS-ANZ

The Joint Accreditation Service of Australia and New Zealand is the IAF member for these countries.

DAC

The Dubai Accreditation Department is a government department that accredits RCBs within the United Arab Emirates.

Other IAF Members

There are over 60 other members of the IAF which provide accreditation services for their respective countries and a full list can be found on the IAF website so when you have a moment why not look up the member organization for your country.

The core message here is that whichever RCB you choose to carry out your certification audit, make sure they are accredited by the IAF member for your country. So for the UK that means UKAS-accredited, the USA ANAB-accredited and so on. Most auditing companies display the logo of the organization that they are accredited by fairly prominently on their website so it should be easy to tell.

Choosing between accredited RCBs

So you've checked that the audit companies you're considering are accredited, but what other factors come into play when making your decision? In our experience asking the following questions will help you to choose:

- *Which standards do they audit?* - Check the RCB has the capability to audit the standard you are going for and if so how many customers they have for that standard. How long have they been auditing the standard and how many qualified people do they have?
- *Do they cover the geographical areas you need?* - There's no point in considering an RCB that can't cover the geographical area(s) you need. This is particularly relevant if you need to have more than one office audited, possibly in different countries. They may cover one country but not another. It's worth checking whether they feel an onsite visit is needed to all of the offices in scope before you dismiss them.
- *How long will it take?*- Officially there is a formula that should be used when calculating how many days an audit should take. This takes into account variables such as number of locations and employees and which standards are involved. However there is some flexibility in how the formula is applied so you may get differing estimates from RCBs on how many days will be needed, which will obviously affect the cost.
- *How much will it cost?* - This follows on from the question about time as most RCBs charge by the hour or day but rates can vary significantly so a longer audit could actually be cheaper. Take into account the ongoing certification fees as well as the cost for the stage one and stage two audits.
- *What is their availability?* - Auditors are generally busy people so if you're in a hurry to get your organization certified then their availability will be an important factor. How soon can they do a stage one and when can they come back for the stage two?
- *What is their reputation?* - Even amongst accredited RCBs, there are more and less well-known names. Since a lot of the reason for going for certification is to gain credibility with your customers and perhaps regulators, consider which RCB would carry most weight with them.
- *How good is their administration?* - A lot of the frustration we see with RCBs is not due to the quality of their auditors but their administration processes. You need an auditing company that will arrange the audits professionally and issue your certificate promptly,

providing additional materials to help you advertise your certification. When you contact them initially, do they return your call and sound knowledgeable?

- *Do they use contract auditors?* - Many RCBs use auditors that are not directly employed by them which is not necessarily a problem, but it would be useful to understand how much continuity you will have with the individuals that carry out your audits. Try to avoid having to describe what your company does to a new auditor every visit as this soaks up time that you are paying for.
- *Do they have experience of your industry?* - Some RCBs and auditors specialize in particular industries and build up a strong knowledge of the issues relevant to their customers. This can be helpful during the audit as basic industry concepts and terms will be understood and time will be saved. Check whether they have audited similar organizations in your industry.

Making a good choice based on the above factors can't guarantee that the certification process will run smoothly, but by having a good understanding of the accreditation regime and by asking the right questions early on you will have given yourself the best chance possible to have a long and happy audit relationship.

Having agreed a price, your chosen external auditor will contact you to arrange the Stage One review. This is essentially a documentation review and a "getting to know you" discussion where the exact scope of potential certification is decided. Based on the Stage One, the external auditor will make a recommendation about your readiness for the Stage Two – the certification audit itself. It used to be common for there to be at least a three month gap between the Stage One and the Stage Two visits but this is less often the case nowadays and the two can be quite close together if desired.

4.2 Are we ready for the audit?

Deciding when to ask the external auditor in for the Stage One visit is a matter of judgement on your part. If you invite them in too early they will simply tell you you're not ready and this can have a detrimental effect on team morale (and possibly cost you more money for further visits). If you leave it longer the danger is that you're extending the timescale to certification unnecessarily. We suggest you use the *ISO/IEC 27001 Gap Assessment and Conformity Action Plan* within the Toolkit as a guide to your readiness, but don't expect to be 100% compliant before going for Stage One. A more appropriate figure is probably 90% or so but it does depend on which areas are not yet complete.

Before arranging the Stage One you should definitely have completed the following:

- Information security policy
- Risk assessment and treatment plan
- Implemented most (but not necessarily all) of your information security controls
- Conducted user awareness training
- Internal audits of all areas of the standard
- At least one management review (ideally more)

Not having any of the above available would probably mean that the Stage One visit is inconclusive in terms of judging your readiness for the Stage Two i.e. the auditor would tell you just weren't ready yet.

4.3 Preparing for audit day

Once you feel you're ready to be visited by the auditor for either the Stage One or Stage Two then there are a number of sensible preparations to take to make the best impression from the start. Firstly, make sure that the visit is confirmed, provide directions and check the time of arrival of the auditor(s). If appropriate, inform reception that he/she will be coming, get an identity badge prepared and reserve a parking space. Book a room for the auditor's use (more if there is a team) and ensure that refreshments will be available, including lunch if possible. You will be needing to show documents and discuss them, so some form of large screen or projector will be useful.

Once the basic arrangements are in place you need to ensure that whoever is going to act as the auditor's guide around the ISMS is ready. This means knowing where all of the relevant documents are and how each of the requirements is met within the documents. Supporting information such as HR and training records should also be available if required. Anyone who might be able to help the auditor such as managers and support staff should be on standby and everyone who is planned to talk to the auditor should be prepared.

There is no substitute for practice so conduct a mock audit beforehand if you can and identify any improvements needed before the day. Having obvious signs of information security-related activity on display at your location does no harm; this could be performance charts or posters for raising awareness on the walls.

It's all about showing the auditor that you are a professional organization that is in control; you may be surprised how little the auditor feels he needs to look at if the overall impression he's getting is very positive.

4.4 At the audit

The auditor should have provided an audit plan which will set out the structure of the audit, including areas to be reviewed, people to be met and timings (this often doesn't happen so don't worry if you don't get one). Despite the appearance of power, auditing is actually quite strictly regulated so the auditor will have specific things he needs to do, in a specific format, starting with an opening meeting and ending with a closing meeting. Do what you can to make it easy for him by providing access to the relevant documents and resources as quickly and smoothly as possible.

Basically all the auditor is doing is the same exercise as you did yourself when you performed (and repeated) the gap assessment. It's purely a matter of going through the requirements of the ISO/IEC 27001 standard and asking to be shown how you meet them. The auditor will need to record the

evidence he has been shown, including any relevant references such as document titles and versions. He may also want to see the relevant procedures etc. in action which may mean reviewing the records you keep and possibly talking to the people who perform the procedures.

If the auditor finds something that doesn't conform to the requirements of the standard, he will raise a "nonconformity". These can be major or minor and, as the names suggest, these vary in importance.

A major nonconformity may be raised if there is a significant deviation from the standard. This is often due to a complete section not really having been addressed, or something important that has been documented but there is no evidence that it has been done. Examples might be if no internal auditing has been carried out, no risk assessment done or no management reviews held.

A minor nonconformity is a lower level issue that doesn't affect the operation of the ISMS as a whole, but means that one or more requirements have not been met. Examples could be that an improvement has not been evaluated properly, a control has not been implemented as planned or a risk assessment doesn't follow the documented process.

Some auditors take note of a third level of item often called an "observation". These are not nonconformities and so don't affect the result of the audit but may be useful for improvement purposes.

Once the audit has been completed the auditor will write up the report, often whilst still on site. He will then tell you the result of the audit and go through any non-conformities that have been raised. Certification to the standard is conditional upon any nonconformities being addressed and upon the higher-level body that regulates the auditors agreeing with his recommendations. This can take a while to process so, even if you have no nonconformities, officially your organization is not certified yet.

You will need to produce an action plan to address the nonconformities and if this is accepted and they are closed off, you will then become certified and the certificate will be issued for a period of three years. During this time, there will be annual surveillance visits followed at the three year mark by a recertification audit.

4.5 After the audit

There is usually a huge amount of pressure built up before the audit and once it's over the relief can be enormous. It's very easy to regard the implementation of a ISMS as a one-off project that is now over. But the auditor will be back within the next twelve months to check that you have carried on running the ISMS as required, so you can't afford to relax too much.

Certification is really a starting point rather than an end result and hopefully as time goes by your ISMS will mature and improve and start to provide more and more value to the organization. However you may find that the resources that were made available for the implementation now start to disappear and you need to ensure that the essential processes of the ISMS are maintained.

Plans can get out of date very quickly so the performance evaluation side of the ISMS in particular will become very important; make sure you continue with the management reviews, exercising and testing controls and internal audits and this should drive the rest of the ISMS to stay up to date.

5 Conclusion

This implementation guide has taken you through the process of putting a ISMS in place for your organization, supported by the CertiKit ISO/IEC 27001 Toolkit. Hopefully you will have seen that most of what's involved is applied common sense, even if the standard doesn't always make it sound that way!

Implementing a management system such as ISO/IEC 27001 is always a culture change towards becoming more proactive as an organization and, with the day to day reactive pressures of delivering a product or service, it can sometimes seem daunting. However we hope you will find that it's well worth the effort as you come to the gradual realization that it's really the only effective way of doing it.

We wish you good luck in your work and, as always, we welcome any feedback you wish to give us via feedback@certikit.com.