
# A Guide to Implementing the ISO20000 Standard

## Contents



## List of Figures

# 1 Introduction

Congratulations on purchasing the CertiKit ISO/IEC 20000 Toolkit. This guide takes you through the process of implementing the ISO/IEC 20000 standard using the document toolkit. It provides a recommended route to certification against the standard starting from a default position where very little is in place. Of course, every organization is different and there are many valid ways to embed the disciplines of IT service management. The best way for you may well depend upon a number of factors, including:

- The size of your organization
- The mix of technologies you use
- Whether you're an in-house or external service provider
- 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
- The legal, regulatory and contractual environment you operate within

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 IT service management; the important thing is that you end up with a Service Management System (SMS) that is relevant and appropriate for your specific organization's needs.

Good luck!

## 1.1 The ISO20000 standard

The ISO/IEC 20000 international standard for "Information technology — Service management – Part 1: Service management system requirements" (referred to in this guide as simply "ISO/IEC 20000") was originally published by the ISO in 2005 and is based upon the earlier British standard BS15000. Revised in 2011 and now in 2018, ISO/IEC 20000 specifies the requirements that your SMS will need to meet in order for your organization to become certified to the standard. The requirements in ISO/IEC 20000 are supplemented by guidance contained in ISO/IEC 20000 Part 2. ISO/IEC 20000 Part 2 is well worth reading as it fills in some of the gaps in understanding how the requirements in ISO/IEC 20000 Part 1 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 20000 series and many of them provide useful supporting information for organizations going for ISO/IEC 20000 certification (or simply using it for guidance). Some of the commonly referenced ones are:

- ISO/IEC 20000 Part 3 – Guidance on scope definition and applicability

- ISO/IEC 20000 Part 5 – Exemplar implementation plan
- ISO/IEC 20000 Part 9 - Guidance on the application of ISO/IEC 20000-1 to cloud services
- ISO/IEC 20000 Part 10 – Concepts and terminology

It's worth pointing out that, although useful, none of these are required reading for ISO/IEC 20000 so if you are limited in time and budget, ISO/IEC 20000 Part 2 is still your best bet.

There's no obligation to go for certification to ISO/IEC 20000 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 IT services effectively.

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. 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/IEC 27001 - Information security management

ISO 22301 - Business continuity 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 ISO/IEC 20000 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 and all new standards or new versions of existing standards will have it. Many other standards have been revised including ISO/IEC 27001 (Information security), ISO22301 (Business continuity management) and ISO14001 (Environmental management).

The good news for an organization implementing an SMS based on ISO20000:2018 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/IEC 27001 at a later date.

The ISO20000 standard consists of a number of major headings which will be common across other standards (because they are the "Annex SL" headings) and 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 "non-conformity" 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 versions of the standards the term "documented information" is generally used instead to cover anything that is recorded (the official 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? Service acceptance tests – what was tested, by whom, when and what was the outcome?

All of this sounds rather onerous, a lot of hassle. True, it can mean more work at least in the short term. But doing service management according to the ISO20000 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 an SMS 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 ISO20000 is that initially you will put things in place because the standard says you will. 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 more benefits 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 ISO20000 Toolkit comes in.

## 1.2 The CertiKit ISO20000 Toolkit

When looking at IT service management the emphasis is usually on the delivery of IT services and the processes used to support them. And it's right that this should be the main focus; it is, after all, the main deliverable of the whole ITSM idea. In a perfect world we would just catalogue our services, put our processes in place and nothing would ever change. The processes would be appropriate and effective at all times, never need improving and everyone would know how to follow 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, services change, people come and go from the organization and our definition of what's important moves all the time.

So, the ISO/IEC 20000 standard proposes that we don't just need a set of processes; we need a *Service Management System* or SMS. The function of the SMS is to wrap itself around the processes (such as incident, change and configuration management) and ensure among other things that:

1. There is ongoing management commitment to the provision of quality IT services
2. Everyone understands what we're trying to achieve and what their role is
3. The IT services continue to meet the business needs
4. We have a good idea of what the current threats to the continuity and security of our services are
5. Everybody knows about the policies, processes and procedures and how to use them
6. We update the processes and associated documentation when things change around it
7. We measure how well we're doing
8. The effectiveness of service delivery gets better over time

The CertiKit ISO/IEC 20000 Toolkit (referred to within this document simply as the "Toolkit") provides not only the processes, but also a large part of the SMS 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® 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. For each of the IT service management processes a policy and a process document is included and these have a common format which helps with consistency.

A document reference naming convention is used throughout the Toolkit which is described in *SMS Documentation Log*. This includes a reference to the section number of the ISO/IEC 20000 standard to which the document applies. 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 [Service Provider] and simple instructions are provided about how to update these.

Every document starts with an "Implementation Guidance" section which describes its purpose, the specific areas of the ISO/IEC 20000 standard it is relevant to, general guidance about completing and reviewing it and some legal wording about licensing etc. Once read, this section may be removed from the final version of the document.

The layout and headings of each document have been designed to guide you 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 processes 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 be aware that other non-highlighted sections may also need to be updated for your organization.

## 1.3 If You're a Small Organization

The CertiKit ISO20000 Toolkit has been deliberately designed to be flexible and easy to adapt to your needs. The standard itself doesn't dictate any specific structure of documentation so you're free to do whatever makes sense for you as long as the requirements are met. Some smaller organizations decide to merge some of the supplied documents together so that the total number of documents in the SMS is reduced. This makes sense if the number of people involved is small and approval cycles are short. To help with this process, you may like to consider incorporating one or more of the following documents into the Service Management Policy:

- Roles Responsibilities and Authorities
- Procedure for the Control of Documented Information
- Procedure for Internal Audits
- Procedure for Management Reviews
- Procedure for the Management of Nonconformity

It's up to each small organization to decide if this approach would be right for them; inevitably there are pros and cons of having more or fewer documents and some form of compromise solution based on our suggestions might also be appropriate.

## 1.4 Where to start

*Relevant Toolkit documents*

- *ISO20000 Gap Assessment Tool*
- *ISO20000 Enhanced Gap Assessment Tool (chargeable extra)*
- *ISO20000 Assessment Evidence*
- *ISO20000 Benefits Presentation*
- *ISO20000 Introduction Presentation*

Before embarking on a project to achieve compliance (and possibly certification) to the ISO20000 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 SMS afterwards) will be successful. Indeed, "Leadership" has its own section within the standard and without it there is a danger that the SMS will not be taken seriously by the rest of the organization and the resources necessary to make it work may not be available.

The first questions top management are likely to ask about a proposal to become certified to the ISO20000 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 ISO20000 Toolkit provides a number of resources.

The ISO20000 Gap Assessment Tool is an Excel workbook that breaks down the sections of the ISO 20000 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 Gap Assessment Tool asks a series of key questions in order to assess how close to meeting the standard your organization is. The questions are designed to address the main requirements of the standard and a positive answer means that you are likely to be conformant.

The Tool includes a variety of tables and charts showing an analysis of where your organization meets the standard and where there is still work to do.

However, if you would prefer to have all of the exact requirements of the standard laid out for you then we provide a further, enhanced tool which is a chargeable extra to the Toolkit and available via the CertiKit website. We are able to provide this because we have a licensing agreement with the ISO, via BSI, to include the full contents of the requirements of the standard (for which CertiKit pays a license fee). The ISO20000 Enhanced Gap Assessment Tool goes several steps further than the default gap assessment by breaking down the text of the ISO20000 standard itself into individual requirements (with the full text of each requirement) 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 ISO20000 Gap Assessment Tool 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 project in order to assess your level of progress from the original starting point.

The accompanying workbook *ISO20000 Assessment Evidence* shows you how the various documents in the Toolkit map onto the requirements and what other evidence may be appropriate to show compliance. 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 *ISO20000 Benefits Presentation* is provided in the Toolkit for this purpose. Note that budgetary proposals should include the costs of running the SMS 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*

- *ISO20000 Project Plan (MS Project)*
- *ISO20000 Project Plan (MS Excel)*
- *Service Management System PID*

- *ISO20000 Progress Report*

Having secured top management commitment, you will now need to plan the implementation of your SMS. 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 ISO20000 Toolkit provides a Microsoft Project® plan as a starting point for your project. 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 could be approached in. This approach, which corresponds to the suggestions in *Part 5 – Exemplar implementation plan* of the ISO20000 standard, is shown in Figure 1 below.

We broadly suggest using a three-phase approach, implementing the reactive aspects of the standard first in order to gain a good degree of control over your service management environment. This can then be followed by the more proactive processes and finally the integration and improvement aspects.

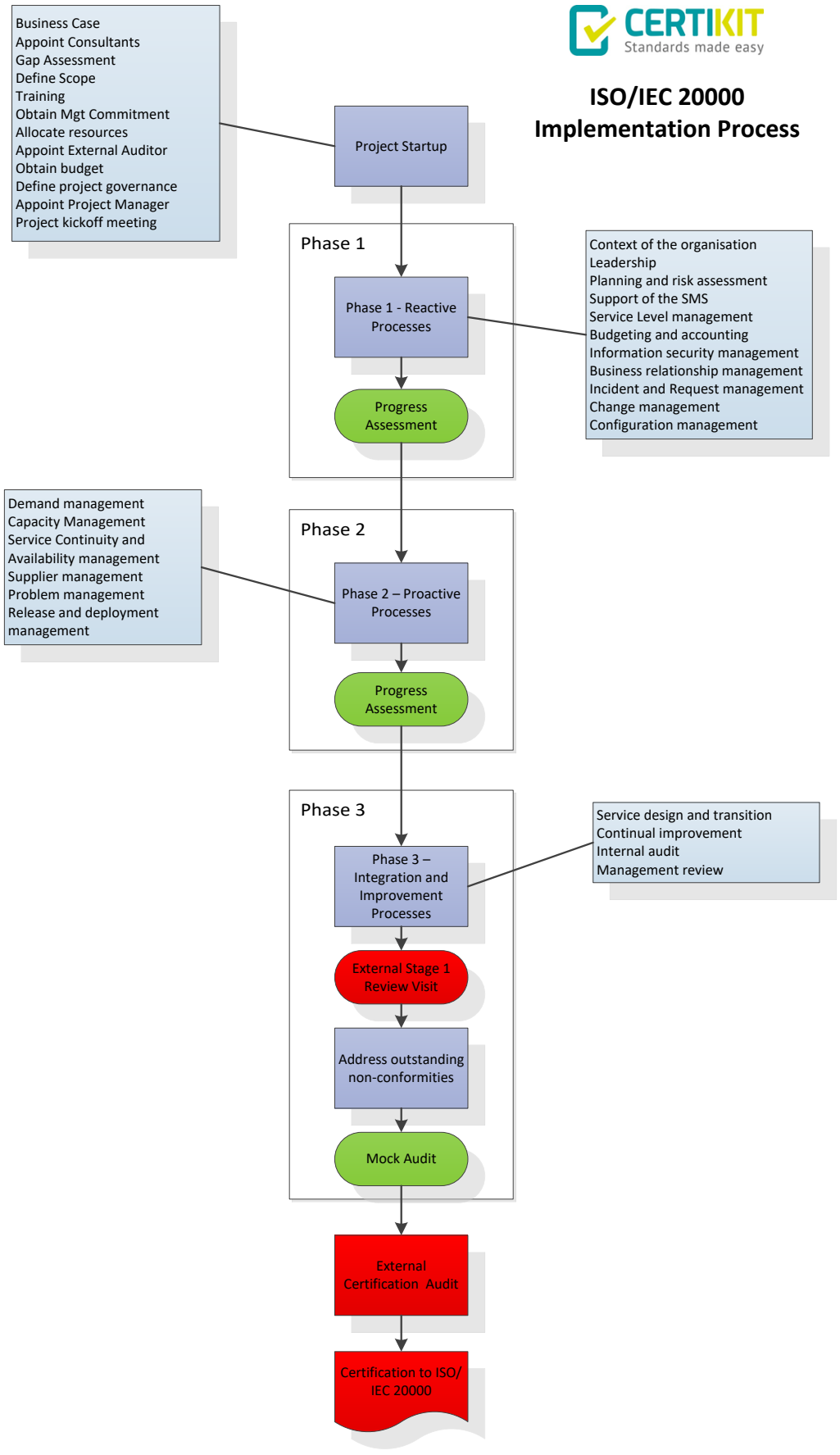


*Figure 1 - A possible implementation approach*

Alternatively, it's fair to say that, in general, if you implement your SMS in the order of the ISO20000 standard from section 4 to section 10 you won't go far wrong.

A simple twelve-step sequence for the route to certification is shown in figure 2 below. As suggested, this effectively steps through the standard in order although it starts with the foundation for the project (and for the ongoing SMS) which is obtaining management commitment.


*Figure 2 – Simple twelve-step project approach*

Whichever approach you decide to take, once a project manager has been appointed and the project has been 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/highlight reports and the CertiKit ISO20000 Toolkit includes a template for such reports.

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 SMS 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 ISO20000 standard one by one, explaining what you may need to do in each area and showing how the various items in the CertiKit ISO20000 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 SMS 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 compliance and hopefully certification. There are many great books available on the subject of service management and we recommend that, if you have time, you invest in a few and supplement your knowledge as much as possible.

# 2 Using the CertiKit ISO20000 Toolkit

The following sections refer to the structure of the ISO20000 standard and how it may be interpreted, including showing how the documents in the Toolkit help to demonstrate conformity. It may help to have a copy of the ISO20000 standard available as you read this section.

## 2.1 Section 0 – Foreword and Introduction

*Relevant Toolkit documents*

- *(None)*

The foreword and the introduction to the standard are worth reading, if only once. Together they give a good summary of what the ISO sees as the key components of an SMS; this is relevant and important when understanding where the auditor is coming from in discussing what might be called the "spirit" of the SMS. 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.

The foreword also sets out the main changes in the 2018 version of the standard compared to the 2011 version.

There are no requirements to be met in this section.

## 2.2 Section 1 – Scope

*Relevant Toolkit documents*

- *(None)*

This section refers to both the scope of the standard and the scope of your SMS. 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. It makes the point that all of the requirements are necessary in order to become certified; you can't become "partially certified" by only performing some of the processes to the required standard. Furthermore, it also explains that the management system must be fully operated by the service provider whereas it is permissible to have some parts of the processes and/or services carried out by a third party as long as the service provider retains control (or "governance") of them.

There are no requirements to be met in this section, but you will need to confirm that the scope of your proposed SMS is allowed under the rules set out here. If you're in any doubt you could refer to Part 3 of ISO/IEC 20000 – *Guidance on scope definition and applicability.*

## 2.3 Section 2 – Normative references

*Relevant Toolkit documents*

- *(None)*

Some standards are supported by other documents which provide further information and are very useful if not essential in using the standard itself. For ISO20000 none are listed.

There are no requirements to be met in this section.

## 2.4 Section 3 – Terms and definitions

*Relevant Toolkit documents*

- *(None)*

Relevant terms and definitions are given in two areas; those specific to management system standards, and those specific to service management. Some of these terms have changed in fairly subtle ways from the 2011 version of the standard. A total of fifty terms and their definitions are listed, many of which are taken from other standards such as ISO9000 and some are broadly based on ITSM frameworks such as ITIL®. It is worth looking back to this section occasionally when reading the standard to get a better idea of what is meant by some of the requirements, although some of the definitions themselves probably require more explanation than is given. The notes included within some definitions can be particularly helpful as they provide further clues about the application of the standard.

There are no requirements to be met in this section.

## 2.5 Section 4 – Context of the organization

*Relevant Toolkit documents*

- *SMS 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 SMS is that it should be appropriate and relevant to the specifics of the business and the services it is being applied to. To ensure this, the people implementing and running the SMS must be able to answer questions about what the organization does, where, how and who for (plus many others).

The SMS 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 SMS. This is particularly relevant when we discuss risk and opportunity assessment 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 SMS 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.

The context section is also the one where the scope of the SMS is defined. This needs careful consideration. If your organization is small, it usually makes sense to place all services it provides 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 service (e.g. the cloud service to customers but not internal systems). It is perfectly acceptable to start with a smaller scope for certification and then widen it out year by year as the SMS 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 SMS and the scope of certification to the ISO20000 standard; they don't have to be the same. You can (if it's useful to do so) have a fairly wide SMS 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*

- *Service Management Policy*
- *Service Management Roles, Responsibilities and Authorities*
- *Top Management Communication Programme*
- *Service Requirements*
- *Executive Support Letter*
- *ISO20000 Service Management System Presentation*
- *Meeting Minutes Template*

The leadership section of the standard is about showing that top management are serious about the SMS 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 SMS 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 SMS 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 a documented top management communication plan, an executive support letter and a template for relevant meetings to be minuted.

The second way for top management to show they are serious about service management is to ensure that there is a policy in place. This needs to be a document, signed off by top management and distributed to everyone that it might be relevant to. A template policy is provided in the Toolkit that addresses the areas required by the standard.

Top management need to make sure that everyone involved in the SMS 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 service management is included in the day to day responsibilities of existing roles rather than trying to create a parallel organization structure just for the SMS; 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*

- *Service Management Plan*
- *Risk Assessment and Treatment Process*

- *Risk Assessment and Treatment Tool*
- *Risk Assessment Report*
- *Risk Treatment Plan*
- *Opportunity Assessment Tool*

Risk and opportunity management is a key principle of ISO20000 and a process for achieving this is provided in the Toolkit, together with a corresponding tool, report and action plan. Although the emphasis is often largely on the potential negative impact of risks, don't forget to look at opportunities too.

A risk assessment needs to be conducted to analyse and evaluate the likelihood of various events occurring, particularly with regard to information security and service continuity. This will then give you the opportunity to do something about those risks that are both likely and have a significant impact. The ISO20000 standard encourages you to become proactive in preventing problems from happening in the first place; obviously if they still do then you will have a plan in place to manage the impact.

There are many ways of analysing risk and, although the ISO20000 standard doesn't explicitly suggest it, another standard, ISO 31000, could 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 service management purposes but for all potential risks to the business. But ISO31000 itself doesn't go into detail about *how* risks should be identified; there is yet another standard that does, which is ISO31010. 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; ISO20000 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 Toolkit provides a risk assessment process which is compatible with the ISO31000 standard. Effective risk identification can often be done by simply getting the right people with the relevant knowledge into 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 Tool* 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 addressed by actions depends upon the risk appetite you decide to adopt. For those risks that do need addressing there are three main options:

1. Mitigate – 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. Transfer – get another party to assume 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 Tool* allows you to define what effect you believe the action 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 actions, some of which may involve spending money. Top management also need to agree to the levels of residual risk after the actions have been implemented (i.e. the risks we're left with once we've done everything proposed).

The key point to remember in addressing 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 method used in the Toolkit is "qualitative" in that it simply categorizes 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 ISO20000 standard.

Within the planning section of the standard we need to set out what the SMS is intended to achieve and how it will be done. With regard to the SMS there are two main levels of objectives. The first is the high-level objectives set out when defining the context of the SMS. These tend to be quite broad and non-specific in order to describe why the SMS 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. The *Service Management Plan* is a key document within the SMS and this section of the standard gives you a long list of things to include within it. The Toolkit document prompts you to describe the various aspects of the plan and to expand on how your SMS will work. The plan should cover a specific timescale and be reviewed on a regular basis. Generally, we would recommend a timeframe of 1-3 years horizon, depending on the size of your organization and the degree of your ambition for your SMS. For example, a one-year plan which is synchronized with the financial year (and hence budgeting cycle) might be appropriate for a small to mid-size company with a fair degree of change to its services and customers. You could, of course, plan the next twelve months in detail and the following 24 months in outline; this would be perfectly acceptable to ISO/IEC 20000.

## 2.8 Section 7 – Support of the service management system

*Relevant Toolkit documents*

- *SMS Documentation Log*
- *Procedure for the Control of Documented Information*
- *Skills and Training Needs Assessment*
- *Meeting Minutes Template*

- *Skills Development Survey*
- *Skills Development Survey Response Analysis*
- *ISO20000 Introduction Presentation*

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

Top management needs to ensure that enough resources are allocated to establish and run the SMS; these may come in many forms, including people (full time and part time), budget (capital and ongoing), information, processing time/space and physical accommodation. A lack of resource will tend to show itself in the missing of reviews, slow rate of improvement, poor customer satisfaction and a general decline of the SMS over time.

With regard to competence and knowledge, the emphasis is on understanding the skills required to run the SMS, whether these skills are currently available in sufficient quantity and then taking action if they are not. The Toolkit provides a skills survey to be performed, the results of which are then collated and analysed, and a set of recommendations reached for improvement. We would suggest you spend some time defining the skills necessary, including asking the opinions of as many interested parties as possible, before running the survey.

The Toolkit provides a method of conducting a survey of the people involved in the implementation and running of the SMS, 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. Note that formal training is not always the answer and that other forms of skills transfer should also be considered.

A template *ISO20000 Introduction 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 SMS may need more in-depth training.

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. Documents and records are key to creating, running and evidencing your SMS and you need to ensure that you have clear, consistent methods of handling them throughout their lifecycle. The standard gives a twelve-point list of documents or document types that should be included in your SMS and you should make sure that you have these. The Toolkit provides a log which may be used to keep track of the documents in your SMS, including their latest version numbers.

The storage, management and approval of documents may be done in any suitable way and the days of needing to print everything and have it signed are long gone. Intranets, document management systems and the humble shared drive are all acceptable ways of storing your documents and electronic signatures are regarded as sufficient for approvals. If you have an existing way of

managing documentation, then there is generally no need to create something new for ISO/IEC 20000.

Records can be more of a challenge as they are often generated by varying systems and procedures in different formats. You will need to review those that are relevant to the SMS and ensure that you know where they are kept and how access to them is controlled.

## 2.9 Section 8 – Operation of the service management system

### *2.9.1 Section 8.1 – Operational planning and control*

*Relevant Toolkit documents*

- *(None)*

As with other similar standards following the Annex SL format, this section of ISO20000 basically duplicates the requirements of several other sections in saying that processes (including outsourced processes) must be controlled, their performance monitored, and records kept.

### *2.9.2 Section 8.2 – Service portfolio*

*Relevant Toolkit documents*

- *Process for Control of Parties Involved in the Service Lifecycle*
- *Service Catalogue*
- *Configuration Management Policy*
- *Configuration Management Process*
- *Configuration Management Procedure*
- *Definitive Media Library Catalogue*
- *Configuration Management Presentation*

If your organization uses one or more internal or external third parties to deliver aspects of some of the processes included in ISO/IEC 20000 then you will need to show that you have retained overall control of these processes for certification purposes. This means that effectively the third party is simply providing the resource to get the job done, not taking over the whole task for you. We suggest that these instances are set out in the *Service Management Policy* and the *Service Management Plan* with references to the relevant contracts and operational level agreements which will show how the relationship works in practice.

Your organization should be the one to decide how the process is designed, carried out and improved. The auditor will expect to see that you are monitoring the performance of the process and the provider on a regular basis, which could involve holding meetings - which of course should be minuted. This is not to say that you shouldn't take account of the experience and feedback of the people performing the process as they may have a better idea of the day to day operation of it and can suggest improvements. Note that we are largely talking here about the processes in section 8 of the standard e.g. incident management or capacity management, not the management system processes in the other sections which must be completely done by the service provider seeking certification.

A good first step in IT service management is to make a list of all of the services that you provide. Include as much information as you can about who the services are provided to, when, how, what hours, main contacts etc. This is the starting point for your service catalogue and we have provided a template in the Toolkit to help in this process. There are a number of ways to create and view a service catalogue for different purposes, but the ISO/IEC 20000 standard simply requires one that includes dependencies between services and service components as a minimum and is agreed with the customer.

The standard requires that configuration information is recorded (usually in a Configuration Management System, CMS) and that it is capable of sharing this information with the change management process. Depending on where your organization is with its software tools at the moment, this can be a technical and financial challenge. Many of the popular service desk systems provide automated tools to capture asset and configuration information on a regular basis and this may be a good place to start. Meeting the requirements in this section without one or more software tools will be difficult unless your IT environment is very small.

However, you will initially need to define what is within the scope of configuration management and what isn't (e.g. do you need to track keyboards and mice?) and this is done within the *Configuration Management Policy* and *Configuration Management Process* documents.

If your organization is in the software development business, then configuration management (and release and deployment management) will be a bigger subject than if it isn't. For non-software businesses the main configuration items will be hardware, software and ideally documentation too and you will need to have procedures to show how new items are created and existing ones are changed or removed.

We have included a *Definitive Media Library Catalogue* to help you to keep track of physical copies of items such as software CD/DVDs and licenses, although if this information can be stored within your CMS then so much the better.

### *2.9.3 Section 8.3 – Relationship and agreement*

*Relevant Toolkit documents*

- *Business Relationship Management Policy*

- *Business Relationship Management Plan*
- *Service Complaint Procedure*
- *User Satisfaction Survey Report*
- *Business Relationship Management Presentation*
- *Service Level Management Policy*
- *Service Level Management Process*
- *Service Level Agreement*
- *Operational Level Agreement*
- *IT Service Card*
- *Service Level Management Presentation*
- *Supplier Management Policy*
- *Supplier Management Process*
- *Supplier and Contracts Database*
- *Supplier Management Presentation*
- *User Satisfaction survey*

Business relationship management is a process that plays an important part in several other processes such as service level management and capacity management by capturing customer requirements on an ongoing basis. This means that first you will need to define who the customers are and then establish a communication mechanism, such as regular meetings, telephone calls, emails etc. with them. The standard is not specific about how such communication will take place but generally it should be appropriate in terms of frequency – often such meetings start as say monthly and then become less frequent according to the perceived need of both parties.

There also needs to be a complaint procedure so that customers have a channel through which to log complaints about services and be satisfied that they are looked at appropriately. Complaints can be relatively rare, so evidence can be lacking for the auditor in this area; some organizations actively encourage complaints (at least in the early days of the SMS) so that the procedure can be used whilst others simply run a test complaint through to verify correct operation.

It is also a requirement of the standard that customer and user satisfaction is measured. There are various ways of doing this; customer satisfaction could be measured during service review meetings or via a survey. User satisfaction is usually measured using a regular survey or as part of a specific process such as incident management. A draft *User Satisfaction Survey* form is included in the Toolkit along with a template report. It is a good idea to share the results of the survey with the users so that they can see that their responses are taken seriously and that improvement actions will result.

Once the service catalogue is agreed, the question of service levels for each service can be addressed via one or more Service Level Agreements (SLAs). The SLA is one of the documents that the auditor will insist upon seeing and he or she will be looking to see that it is in final version and has been agreed by the appropriate parties. If it isn't, this is likely to lead to a non-conformity being raised so it's important to ensure it is in place – again a template is provided.

Once your service catalogue and SLA(s) are in place it's really a case of keeping them up to date with changes that happen within your organization and the services in order to ensure compliance. You'll also need to monitor whether service targets are being met and do something about it if they are not.

Where you have an arrangement for an internal group to provide some element of service, this must be set out in an *Operational Level Agreement* (OLA). These are generally very similar in nature to an SLA and a template is provided.

A *Supplier and Contracts Database* is a good way of obtaining and maintaining control of the wide variety of suppliers that even the smallest IT service provider generally deals with. This will help to understand what goods and services are purchased, how much they cost, what the contractual commitment is and even whether a formal contract exists at all. The ISO/IEC 20000 standard includes a list of the items that should be included in each contract, although for larger suppliers, if all of these items are not included in their standard contract, it may be difficult to have them added (most auditors accept this).

The *Supplier Management Process* shows how to categorize your suppliers and then arrange regular communication and review accordingly. You will need to ensure that all meetings with suppliers are minuted and that where service targets are set, these are monitored and reviewed regularly.

### *2.9.4 Section 8.4 – Supply and demand*

*Relevant Toolkit documents*

- *Budgeting and Accounting for Services Policy*
- *Budgeting and Accounting for Services Process*
- *Service Costing Model*
- *Budgeting and Accounting for Services Presentation*
- *Capacity Management Policy*
- *Capacity Management Process*
- *Capacity Plan*
- *Capacity Management Presentation*

The ISO/IEC 20000 standard requires that the financial aspects of service management are under control with defined budgets which have expenditure against them tracked and monitored. This is often the case under normal financial rules for all but the smallest organization anyway, so parts of the requirements typically don't require additional work – the IT function usually has a budget allocated to it by default.

However, the standard also suggests that costs be allocated to specific services and this is often a new idea which requires a fair degree of thought. The intention is to understand how much a service costs to provide as a basis for possible comparison with alternative methods of provision, and to see

whether the business benefit is worth the cost. It is likely that the resulting model will only ever be a rough estimate at best because the interconnectedness of IT services and the blurred lines between them mean that it is hard to allocate costs to services accurately, but it's an interesting exercise to do, so give it a try. We provide an outline *Service Costing Model* to illustrate the kind of approach to take.

For demand and capacity management, these fairly short sections of the standard basically say that you must have a capacity plan. However, the plan needs to cover not only technical resources such as server processing, disk space and network bandwidth but also people, information and finances – the intention is that you look at all of the areas necessary to run a service, not just the infrastructure.

The Toolkit includes a *Capacity Plan* that covers the required areas. Our recommendation would be that you concentrate initially on all aspects of your most critical services before expanding the scope of your capacity management to other, less vital services.

Advance notice of capacity requirements should come from your meetings with interested parties as part of your business relationship management process and from the implications of proposed changes.

The standard also requires that you monitor capacity usage and tune performance. For technical resources this is often best done using a software tool as doing it manually will take too much time. This information can then be used to look at the tuning of those resources to ensure that you're getting the most from your investments.

### *2.9.5 Section 8.5 – Service design, build and transition*

*Relevant Toolkit documents*

- *Change Management Policy*
- *Change Management Process*
- *Change Management Presentation*
- *Design and Transition of New or Changed Services Process*
- *Business Case*
- *Project Initiation Document*
- *Service Requirements Specification*
- *Service Design Specification*
- *Project Post Implementation Review*
- *Design and Transition of New or Changed Services Presentation*
- *Release and Deployment Management Policy*
- *Release and Deployment Management Process*
- *Release and Deployment Plan*
- *Software Catalogue*
- *Release and Deployment Management Presentation*
- *Change Request Form*

- *Service Acceptance Checklist*
- *Project RAID Log*
- *Project Progress Report*

The change management process underpins a number of other processes and acts as a co-ordinating influence across the SMS. The *Change Management Policy* defines under what circumstances a change will be considered appropriate to go through the design and transition of new or changed services process and be managed as a project.

The *Change Management Process* sets out the flow of the various types of change and it may be appropriate to use this as the basis of a software workflow system that implements the process (depending on the tools you have available).

The auditor will want to see some example change records to trace them through the process to ensure that they were raised, assessed, approved, implemented and reviewed correctly. They should also be linked to any associated incident, problem, configuration and release records.

It's important to be clear about the circumstances in which the design and transition of new or changed services process will be used, since it involves a degree of control and oversight that a smaller change does not. The standard says that every change, including large ones, should be controlled via the change management process and so even a major project would have a change number within the change management process or system. However, for changes "with the potential to have a major impact on services or the customer" the implementation generally needs to be planned in more detail, with requirements, design and acceptance defined carefully and reviewed by a wider audience. These are therefore better managed within a project environment.

Within the Toolkit, the criteria that make a change a project rather than a normal change are defined in the *Change Management Policy* and you will need to adjust these criteria to match your organization's expectations. The overall path to be followed for a major change is set out in the *Design and Transition of New or Changed Services Process*. When creating the SMS it will not generally be expected that projects that are in the closing stages of delivery will necessarily comply with this process, but the auditor will want to see that anything that was started after the SMS came into being has been managed accordingly, and evidence of requirements gathering, design and acceptance testing are available for review.

A number of documents are provided in the Toolkit to help to manage a major change as a project, starting with the *Business Case* which may need to be created and approved before the project is formed. The *Project Initiation Document* is then defined, and the project will go through requirements, design, acceptance and transition before becoming a new or changed service. The *Service Requirements Specification* document within the Toolkit provides a way of documenting the service-related attributes of the new or changed service.

The progress of the project will be reported upon using the *Project Highlight Report* and its Risks, Actions, Issues and Decisions tracked using the *Project RAID Log*.

The important thing to remember when considering design and development within the context of the ISO/IEC 20000 standard is that it deals with *services*, rather than systems or applications. Although new applications should be designed and developed to meet the users' functional needs, this sometimes doesn't address the service management needs such as incident management, roles and responsibilities, service levels and capacity. The focus for compliance to the ISO/IEC 20000 standard is therefore on support requirements and how the new service will be incorporated into the existing service management environment. Otherwise the SMS would simply become more and more out of date as further services were introduced and changed. The *Service Design Specification* document within the Toolkit ensures that these areas (and others) are fully considered during the design stage.

It is important that the new service is tested before being accepted for implementation and a *Service Acceptance Checklist* is provided for this purpose. This will usually be one of a number of types of testing carried out, such as user acceptance and integration testing.

Since the new or changed service is still under the control of the change management process, a *Release and Deployment Plan* will be created to transition it into live running. Once live and stable, a *Post-Project Implementation Review* will be carried out to identify lessons learned.

If your organization writes its own software, then the expectations of the auditor will most likely be higher in this area than if it purely makes use of commercial off the shelf software (COTS). For those simply using COTS the emphasis will be on customer liaison and testing whereas for those writing bespoke code there will also be development and release definition issues.

However, in both cases, the starting point is to define and agree the frequency and types of releases and then to plan for them effectively. The general approach is set out in the *Release and Deployment Management Policy* with more detail described in the *Release and Deployment Management Process*.

The details of each specific release will be set out in a *Release and Deployment Plan* which sets out the way in which a release will be deployed, including the configuration items, training, testing and timing involved.

The release and deployment process works closely with the change management and configuration management processes and for small organizations many of the requirements in this section may be met by using well-defined procedures in these areas.

### *2.9.6 Section 8.6 – Resolution and fulfilment*

*Relevant Toolkit documents*

- *Incident Management Policy*
- *Incident Management Process*
- *Major Incident Management Process*
- *Service Request Management Policy*

- *Service Request Management Process*
- *Incident and Request Management Presentation*
- *Problem Management Policy*
- *Problem Management Process*
- *Problem Management Presentation*
- *Incident Model*
- *Request Model*
- *Major Incident Report*
- *Problem Dashboard*
- *Major Problem Report*

Incident management is rarely a new process to organizations looking to comply with ISO/IEC 20000, so this is really a case of adjusting your existing process to make sure it meets the requirements. Key changes may be to make sure that the incident management process (often implemented via the service desk function) has access to information from other processes such as known errors, problem resolutions and the CMS.

As well as the relevant policy and process documents, we have also included an *Incident Model* and *Request Model* within the Toolkit. These may help in defining the information required for new incidents and service requests.

A *Major Incident Management Process* is required, and you will need to ensure that this interfaces well with your service continuity procedures.

Effective problem management can give a great return on investment if done well and most if not all of the requirements in the ISO/IEC 20000 standard are met by following the *Problem Management Process* as provided in the Toolkit. The auditor will be looking to see if there is adequate management support for the problem management process and that problems are seen through to resolution. A *Problem Dashboard* report is included in order to raise the profile of problem management and emphasize its benefits.

You may need to look at the IT service management system in use to determine whether it supports the logging of problems (and other records such as changes and releases). If not, often systems can be reconfigured to provide such functionality, or it could be time to look at replacing the current system with one that provides support for a wider range of processes.

### *2.9.7 Section 8.7 – Service assurance*

*Relevant Toolkit documents*

- *Service Continuity and Availability Management Policy*
- *Business Impact Analysis Process*
- *Service Continuity Plan*

- *Service Continuity Test Plan*
- *Service Continuity Test Report*
- *Availability Management Plan*
- *Backup Policy*
- *Incident Response Procedure*
- *Service Continuity and Availability Management Presentation*
- *Information Security Policy*
- *Risk Assessment and Treatment Process*
- *Risk Assessment Report*
- *Risk Treatment Plan*
- *Information Security Summary Card*
- *Information Security Management Presentation*
- *External Organization Information Security Agreement*
- *User Access Management Process*
- *Data Centre Access Procedure*
- *Business Impact Analysis Tool*
- *Post Incident Report*
- *Risk Assessment and Treatment Tool*
- *Personal Commitment Statement*

If we focus on the main service availability and continuity requirements in this section of the standard, they are that you must have performed a risk assessment, you must have a service continuity plan, it must be based on an understanding of customer requirements and you must be testing the plan on a regular basis. If any of these four are not in place you are likely to receive a non-conformity from an auditor.

In the Toolkit we go a little further by providing a method for business impact analysis, which is not strictly required by the ISO/IEC 20000 standard, but we believe it's the best way to establish customer requirements properly.

By looking at your service catalogue and talking to your customers (and based on your own "gut feel" from running the services) you should be able to identify the most critical services that you provide. If you can run a full business impact analysis exercise with your customers, then that's even better as it will highlight the non-IT resources that are also required during a disruptive incident.

You should then be in a position to conduct a risk assessment using the *Risk Assessment and Treatment Process* and *Risk Assessment and Treatment Tool*, looking at the impact and likelihood of various threats to these services occurring, giving you a risk score and associated grading of high, medium or low. Decisions then need to be made about what to do about risks that are unacceptable to you. Now, the ISO/IEC 20000 standard has requirements for both service continuity and availability in this section. In general terms, actions you can take to mitigate some of your risks should be included in your *Availability Management Plan* – this is about being proactive and preventing things happening in the first place. For the others, where you need to plan for the risk actually occurring, you will need a *Service Continuity Plan*. We have also included in the Toolkit an

*Incident Response Procedure* which is intended to help with the management and co-ordination of the organization-wide response to a disruptive incident. This response may involve invoking one or more of the service continuity plans.

Once in place the plans need to be tested to ensure that they work and to identify any improvements that can be made. You will also need to keep them up to date as the organization and its IT services change. The change management process will need to flag up when a change has an effect on service continuity plans; in an extreme case, even a small change can mean that a service continuity plan no longer works in practice.

All tests need to be recorded and a review conducted whenever the plans are used – documents are included in the Toolkit for these actions.

Information security is a big area that has an international standard all of its own (ISO/IEC 27001) but the ISO/IEC 20000 standard does a good job of summarizing the important points in a relatively short space.

Firstly, you must have an information security policy that has been approved and communicated to everyone that should see it. Generally, most organizations take one of two approaches to policy creation; they either go for a single 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 (and one is provided in the Toolkit); 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. For this reason, you may want to consider dividing the supplied document into individual policies.

There isn't a single right answer for the information security policy in the context of the ISO/IEC 20000 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.

You will also need to conduct a risk assessment and then select controls to address your unacceptable risks. For a full list of reference controls, you could refer to the ISO/IEC 27001 standard Annex A (this is useful, but not required by ISO20000). The information security risk assessment process will largely be the same as for a service continuity risk assessment.

As with service continuity and capacity, changes should be assessed for information security implications. Security incidents will be managed using the normal incident management process, but staff involved in investigation may need to be aware of the rules involving the preservation of digital evidence if the perpetrator of a breach is ever to be prosecuted.

## 2.10 Section 9 – Performance evaluation

*Relevant Toolkit documents*

- *Process for Monitoring Measurement Analysis and Evaluation*
- *Procedure for Service Management Audits*
- *Service Management System Audit Plan*
- *Internal Audit Report*
- *Service Management System Review Spreadsheet*
- *Service Management Review Meeting Agenda*
- *Service Reporting Policy*
- *Service Report*
- *Internal Audit Action Plan*
- *Internal Audit Checklist*
- *Internal Audit Schedule*

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

### *2.10.1 Monitoring, measurement, analysis and evaluation*

The ISO20000 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 SMS 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 SMS 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 recorded 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 SMS 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 SMS.

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 SMS 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 SMS.

The Toolkit has a number of documents to help with the internal auditing process, including a schedule, plan, procedure 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 SMS which, if you get it right, will hold together everything else and make audits (internal and external) a relatively straightforward experience. The ISO20000 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 SMS. 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 SMS 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. The Toolkit has a procedure and a sample agenda for a management review.

### *2.10.4 Service reporting*

Following on from the creation of one or more SLAs, you will need to report against the metrics you have stated in order to show whether the service levels are being delivered. The standard gives a list of six areas that should be reported against and a template report is included in the Toolkit.

The standard requires that a description of each report be documented and although this initially seems a little excessive you will undoubtedly find it very useful – if a report is only generated every month or quarter then it can be very easy to forget how you did it last time and if you do it slightly differently each time then comparisons and trends won't be valid.

The frequency of reporting is often a compromise between the expectations of the customer and the amount of work involved in creating a report. Monthly service reporting is good, but you may find that quarterly is sufficient, particularly for stable services that have been in place for a while. The auditor will expect to see at least one service report and ideally several.

As well as reports to the customer, you will need to produce further internal reports to help in the day to day management of the processes. An example would be the number of incidents being opened and closed per week and perhaps a report on the performance of individual members of your incident management team. These may be needed more frequently than service reports so that you can take action as soon as required.

## 2.11 Section 10 - Improvement

*Relevant Toolkit documents*

- *Procedure for Continual Service Improvement*
- *Service Improvement Plan*
- *Procedure for the Management of Nonconformity*
- *Nonconformity and Corrective Action Log*

The ISO definition of a non-conformity 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.

Continual improvement is a key theme of ISO20000 and the standard requires that opportunities for improvement are identified, approved, documented, fully defined in terms of targets, priority and plans and then tracked through to implementation and later review. Ideas for improvement may come from many sources, including users, customers, suppliers, IT staff and other interested parties and it's important to be able to recognise them as improvements and get them recorded.

# 3 Advice for the Audit

## 3.1 Choosing an Auditor

If your organization wishes to become certified to the ISO20000 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 ISO9001 then it usually makes sense to use the same auditing company for ISO20000, 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 ISO20000 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. 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 ISO20000").

***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.

## 3.2 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 *ISO20000 Gap Assessment Tool* 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:

- Service management policy
- Service management objectives and plan to achieve them
- Risk and opportunity assessments
- All of the required processes are in place, at least in basic terms
- 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.

## 3.3 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 SMS 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 individual process managers 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 service management-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.

## 3.4 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 ISO20000 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 "non-conformity". These can be major or minor and, as the names suggest, these vary in importance.

A major non-conformity may be raised if there is a significant deviation from the standard. This is often due to a complete section or process 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 non-conformity is a lower level issue that doesn't affect the operation of the SMS 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 procedure has not been carried out as specified 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 non-conformities 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 non-conformities 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 non-conformities, officially your organization is not certified yet.

You will need to produce an action plan to address the non-conformities 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.

## 3.5 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 SMS 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 SMS 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 SMS 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 SMS are maintained. Plans can get out of date very quickly so the performance evaluation side of the SMS in particular will become very important; make sure you continue with the management reviews, performance monitoring and internal audits and this should drive the rest of the SMS to stay up to date.

# 4 Conclusion

This implementation guide has taken you through the process of putting a SMS in place for your organization, supported by the CertiKit ISO20000 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 ISO20000 is always a culture change towards becoming more proactive as an organization and, with the day to day reactive pressures of delivering IT services, 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.