Understanding the New ISO Management System Requirements

David Brewer

bsi.

Understanding the New ISO Management System Requirements

Understanding the New ISO Management System Requirements

David Brewer

bsi.

First published in the UK in 2014

by
BSI Standards Limited
389 Chiswick High Road
London W4 4AL

©The British Standards Institution 2014

All rights reserved. Except as permitted under the Copyright, Designs and Patents Act 1988, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior permission in writing from the publisher.

Whilst every care has been taken in developing and compiling this publication, BSI accepts no liability for any loss or damage caused, arising directly or indirectly in connection with reliance on its contents except to the extent that such liability may not be excluded in law.

While every effort has been made to trace all copyright holders, anyone claiming copyright should get in touch with the BSI at the above address.

BSI has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this book, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

The right of Dr David Brewer to be identified as the author of this Work has been asserted by him in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

Typeset in Great Britain by Letterpart Limited, www.letterpart.com
Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978-0-580-82166-0

Contents

Foreword

In April 2012, ISO updated its directives. In particular, there is a new annex – Annex SL – in which Appendix 3 defines the high level structure and identical core text for all new and revised management system standards[1]. The concept is that some requirements, e.g. management review, are common to all management system standards and therefore ought to be identically worded.

Several management system standards have now been published in conformance with these new directives (e.g. ISO 22301:2012 on business continuity and ISO/IEC 27001:2013 on information security) while others are being revised (e.g. ISO 9001 on quality).

The identical core text is very good at defining the essential features of a management system and does so without constraining organizations to do things in a particular way, which some organizations may have felt to be inappropriate or bureaucratic. Moreover, familiar concepts such as PLAN-DO-CHECK-ACT and preventive action have disappeared and have been replaced by new ones. The overall goal is to make it easier to create integrated management systems and to adapt management system standards to the nature and culture of organizations.

The aim of this book is to explain the new requirements and how they are related to those in management system standards published prior to the advent of the new ISO directives; to show how familiar concepts have metamorphosed into new ones; and to give fresh insights into understanding management system standards. The book gives guidance on how to develop a management system for the first time. It gives advice on transitioning existing management systems to the new identical core requirements and on integrated management systems.

This book has been designed so that you can read it from cover to cover to gain a comprehensive understanding of the new standard, and then later use it as a reference book.

I have over 30 years' worldwide experience in working with management systems as a standards maker, consultant, auditor, tutor and management system administrator, the past several years running a number of integrated management systems. Many of the insights that I share with

[1] This is correct for the 3rd edition. However, in July 2013, ISO published the 4th Edition, in which Appendix 3 has become Appendix 2.

you in this book are derived from this practical experience, supplemented by the insights afforded by being a member of the international ISO/IEC 27001:2013 development team, where one of the tasks was to achieve consensus and conformity with Annex SL.

This book is a 'must-have' for organizations and individuals keen on ensuring a smooth transition and obtaining maximum benefit from their investment in having a management system.

David Brewer

Acknowledgements

Figures 2, 3, and 4 have been reproduced by kind permission of IMS – Smart Limited.

Chapter 1 – The new ISO management system requirements

Introduction

Since April 2012 all new and revised management system standards must conform to new rules regarding the structure and content of management system standards. These rules are documented in Annex SL, Appendix 3 to the ISO/IEC Directives, *Part 1 — Consolidated ISO Supplement*, referred to as Annex SL for short. In essence, Annex SL specifies the high level structure, identical core text, common terms and core definitions that form the nucleus of future and revised ISO management system requirements standards. Individual management systems standards add additional 'discipline-specific' requirements as required. Because of the newness of Annex SL some deviations are permitted. The remainder of this chapter is laid out in the following subsections:

1. Motivation;
2. High level structure;
3. Identical core text;
4. Deviations; and
5. Discipline-specific text.

Motivation

The objective is to ensure that when a requirement ought to be common to more than one management system standard then it is identically worded. This has benefits when an organization wishes to have a single management system (often referred to as an integrated management system) that conforms to more than one management system standard. For example an integrated management system might conform to ISO 9001 (on quality), ISO/IEC 27001 (regarding information security) and ISO 22301 (on business continuity). In this case (once all three standards conform to the new directives) the core requirements, say for documented information, will be identically worded.

Prior to Annex SL, the need for compatibility was not necessarily fully appreciated by standards developers. ISO/IEC 27001:2005, *Information Security Management Systems*, for example, was developed from

BS 7799-2:2002 using the ISO 'Fast Track' procedure. BS 7799-2:2002 was itself developed by a core team of five people, who were encouraged by BSI to adopt the principles of ISO 9001:2000. At the time, the concept of an integrated management system was a gleam in BSI's eye, and certainly no organization to the knowledge of that core team had one. They adopted the PLAN-DO-CHECK-ACT concept and used it to structure Section 4 of their standard covering all of what they regarded as the information security management system requirements. They then added five additional sections (documentation requirements, management responsibility, internal audits, management review and improvement), modelling them on the corresponding sections in ISO 9001:2000. The word 'modelling' is key. Requirements were taken from ISO 9001:2000 and then changed, sometimes quite subtly. For example, in ISO 9001:2000 Subclause 4.2.3f) states 'to ensure that documents of external origin are identified and their distribution controlled' became, in ISO/IEC 27001:2005, 4.3.2g) 'ensure that documents of external origin are identified' and 4.3.2h) 'ensure that the distribution of documents is controlled'. In ISO 9001:2000 control of distribution only applies to documents of external origin. In ISO/IEC 27001:2005 control of distribution applies to all documents. From an integrated management perspective, there are therefore two issues: organizations must read both standards very carefully in order to identify such differences; and organizations must make a choice. In this case it is to apply the distribution requirement to all documents within scope of the integrated management system, or only apply to information security related documents.

The choice is not necessarily straightforward as some documents could contain elements that are quality and information security related. Choice of option b) could leave one wondering whether a document should be controlled or not; whereas choice of option a) could mean much retrospective work if the quality management system existed first. To simply ignore the difference ought to, of course, lead to a nonconformity.

Despite such subtle differences, it is fortunate that ISO/IEC 27001:2005 is modelled on ISO 9001:2000. This is not the case for all management system standards issued prior to April 2012. ISO/IEC 20000-1:2005, *Information technology — Service management*, has an entirely different structure. So much so, that a whole standard, ISO/IEC 27013:2012, *Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*, has been developed to show how ISO/IEC 20000-1:2011 can be integrated with ISO/IEC 27001:2005.

Such integration issues and the need for additional standards ought to become regarded as a quaint piece of history with the advent of Annex SL.

High level structure

The high level structure for all new and revised management system standards is:

0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organization
  4.1 Understanding the organization and its context
  4.2 Understanding the needs and expectations of interested parties
  4.3 Determining the scope of the XXX management system
  4.4 XXX management system
5 Leadership
  5.1 Leadership and commitment
  5.2 Policy
  5.3 Organization roles, responsibilities and authorities
6 Planning
  6.1 Actions to address risks and opportunities
  6.2 XXX objectives and planning to achieve them
7 Support
  7.1 Resources
  7.2 Competence
  7.3 Awareness
  7.4 Communication
  7.5 Documented information
    7.5.1 General
    7.5.2 Creating and updating
    7.5.3 Control of documented information
8 Operation
  8.1 Operational planning and control
9 Performance evaluation
  9.1 Monitoring, measurement, analysis and evaluation
  9.2 Internal audit
  9.3 Management review
10 Improvement
  10.1 Nonconformity and corrective action
  10.2 Continual improvement

Note that here, and throughout this book, 'XXX' is used to represent the discipline that is the subject of the management system standard. Thus, for ISO 9001, XXX = quality, for ISO/IEC 27001, XXX = information security, etc.

Identical core text

The requirements that are identical to all new and revised management system standards are known collectively as the identical core text.

As an aid to readability, some identical core requirements are prefaced by the subject name of the standard, e.g. the words 'quality' or 'information security'. These requirements are not quality or information security-specific. While the identical core text is the subject of this book, a good way to tell upon reading a management system standard is to change the discipline word(s) (e.g. read 'information security' instead of 'quality') and see if the requirement is still meaningful. If it is, there is a good chance that it is an identical core requirement.

Deviations

A deviation is where a management system standard changes the identical core text by:

1. deleting it;
2. adding text which is not discipline-specific (i.e. the requirement can apply to all management systems, regardless of discipline); or
3. moving it.

Deviations have been permitted to allow the standards developers to overcome problems when a discipline-specific requirement contradicts an identical core text requirement. The intention was not to allow standards developers to change the identical core text just because they did not like it or felt they could say it better. For this reason, all deviations have to be justified.

It should be noted that ISO 22301:2012, *Societal security – Business continuity management systems – Requirements*, was developed at a time when Annex SL was itself in development. There are therefore requirements in that standard that appear to be deviations but are in fact identical core text from an earlier version of Annex SL.

Discipline-specific text

Requirements that are specific to a particular discipline (e.g. information security) are referred to collectively as discipline-specific text. Such text may be embedded into the identical core text. For example, ISO/IEC 27001 has requirements for risk management. In ISO/IEC 27001:2013, these discipline-specific requirements are primarily in Subclauses 6.1.2, 6.1.3, 8.2 and 8.2, but there are discipline-specific matters that a management review must attend to and these have been inserted into a list in the identical core text of Subclause 9.3. Note that

the insertion of text can modify the clause numbering. In ISO/IEC 27001:2013, for example, the insertion of Subclauses 6.1.2 and 6.1.3 causes the identical core text of Subclause 6.1 to become 6.1.1.

The amount of discipline-specific text varies between standards. In ISO 22301:2012, for example, there is approximately four-and-a-half pages of discipline-specific text in Clause 8, which specifies in detail the requirements concerning business impact analysis, risk assessment, strategy, procedures, exercising and testing. Likewise one might expect the revised version of ISO 9001 to contain about five pages of discipline-specific text also in Clause 8, corresponding to the 'product-realization' requirements which are currently in Clause 7 of ISO 9001:2008. In contrast, ISO/IEC 27001:2013 only has about two pages of discipline-specific text, mostly located in Clause 6. This is because ISO/IEC 27001 traditionally deals with information security controls in an annex, which is actually quite long – 13 pages.

Chapter 2 – Management system concepts

Introduction

The objective of this chapter is to facilitate an understanding of management system concepts. The chapter is laid out in the following sections:

1. definition of terms used in Annex SL;
2. an explanation of what a management system is;
3. an explanation of how a management system works;
4. an explanation of how to read and interpret management system standards;
5. an explanation of how management system concepts have evolved; and
6. an introduction to integrated management systems.

Definitions

Overview

Annex SL defines a variety of terms that are fundamental to understanding management system concepts in general and the identical core text in particular. If a term is not defined in Annex SL, then the definition given in the Oxford English Dictionary (OED) is to be used. It is important to use these definitions, otherwise there is a risk of misunderstanding the requirements of the standard. Management system standards may add additional terms. If a management system standard alters an Annex SL definition, then it is treated as a deviation. For example, both ISO 22301:2012 and ISO/IEC 27001:2013 use the ISO Guide 73 definition of risk (i.e. the 'effect of uncertainty on objectives') as opposed to the Annex SL definition (which is just the 'effect of uncertainty').

The definitions are reproduced and discussed here in three groups:

1. terms relating to the management system;
2. term relating to documented information; and
3. other terms.

Terms relating to the management system

The Annex SL definitions are:

management system: set of interrelated or interacting elements of an **organization** to establish **policies** and **objective**s and **processes** to achieve those objectives

organization: person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its **objectives**

top management: person or group of people who directs and controls an **organization** at the highest level

policy: intentions and direction of an **organization** as formally expressed by its top management

objective: result to be achieved

process: set of interrelated or interacting activities which transforms inputs into outputs

It is important to appreciate that an organization does not have to be a company. Indeed there is a note in Annex SL, which says 'The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private'. It therefore follows that if the organization is part of a larger organization then:

1. from the perspective of the smaller organization the larger organization is referred to either as 'another organization' or an 'external organization', the two phrases being synonymous with one another; and
2. top management refers to the leader of the smaller organization, not to the leaders of the larger organization.

This relationship is illustrated in Figure 1.

Term relating to documented information

The Annex SL definition is:

documented information: information required to be controlled and maintained by an **organization** and the medium on which it is contained

Documented information is a new term that has been traditionally referred to as documentation and records. A good way to think of this is that there are two types of documented information: *specifications* (Type

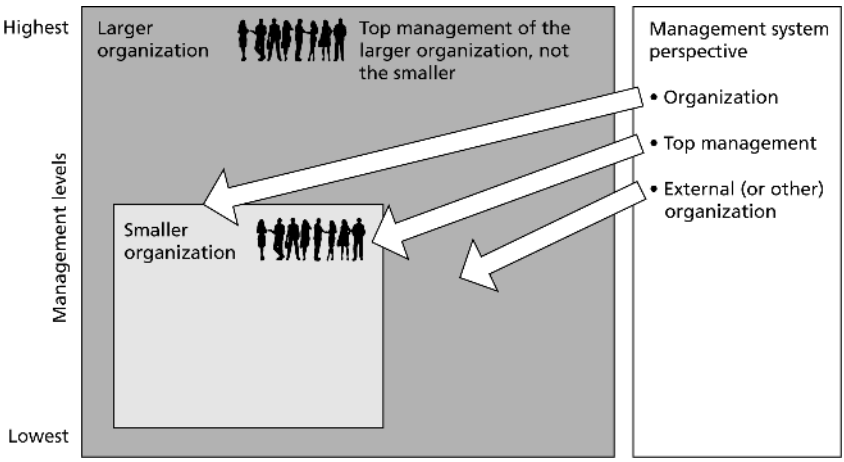

Figure 1: The organization may be part of a larger organization

S), which specify what an organization intends to do (i.e. in the future) and *records of performance* (Type P), which record what has happened (i.e. in the past). As an item of documentation, e.g. a web page, it could contain both types; ISO has decided to use a single term to cover both documentation and records.

It is also important to note that it ought to be very rare that a management system standard gives names to documents. Subclause 5.2 starts by stating 'Top management shall establish an XXX policy' and continues by requiring that policy to have certain characteristics, e.g. it includes a commitment to continual improvement of the management system. The subclause also states that the policy 'be available as documented information'. This is not a requirement to have a document called 'XXX Policy'. It is a requirement that the information specified in Subclause 5.2 be documented. How an organization does this, and how it wants to refer to it, is up to the organization to decide and no one else. It could, for example, put the information required by Subclause 5.2 together with other information (whether required elsewhere by the standard or not) on an intranet web page entitled Integrated Management System Policy.

Other terms

Other Annex SL definitions are:

interested party (preferred term), **stakeholder** (admitted term): person or **organization** that can affect, be affected by or perceive themselves to be affected by a decision or activity

requirement: need or expectation that is stated, generally implied or obligatory

effectiveness: extent to which planned activities are realized and planned results are achieved

risk: effect of uncertainty on **objectives**

competence: ability to apply knowledge and skills to achieve intended results

performance: measurable result

outsource: make an arrangement where an external **organization** performs part of an organization's function or **process**

monitoring: determining the status of a system, a **process** or an activity

measurement: **process** to determine a value

audit: systematic, independent and documented **process** for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

conformity: fulfilment of a **requirement**

nonconformity: non-fulfilment of a **requirement**

correction: action to eliminate a detected **nonconformity**

corrective action: action to eliminate the cause of a **nonconformity** and to prevent recurrence

continual improvement: recurring activity to enhance **performance**

Oxford English Dictionary terms

There are a number of terms that are not defined by Annex SL and therefore they take on a meaning as defined by the Oxford English Dictionary (OED). Those whose meanings are used in this book are reproduced below:

issue (OED): an important topic or problem for debate or discussion

scope (OED): the extent of the area or subject matter that something deals with or to which it is relevant

activity (OED): a thing that a person or group does or has done

function (OED): an **activity** that is natural to or the purpose of a person or thing

status (OED): the situation at a particular time during a **process**

plan (OED): a detailed proposal for doing or achieving something

What is a management system?

In order to gain further insight into the definition of a management system, consider the following.

1. The OED provides a number of meanings for the word 'of', the most relevant of which is 'indicating an association between two entities, typically one of belonging, in which the first is the head of the phrase and the second is something associated with it'. Thus, for example, one might say 'the information security policy *of ABC* incorporated'.
2. There will be people within the organization that will establish policy. Indeed, top management is responsible for establishing the XXX policy (see Subclause 5.2). However, if a management system was only made up of people, the definition would say 'a person or group of people with the organization that establishes …'. The definition does not refer to people. Instead it refers to 'interrelated or interacting elements'.
3. An 'element', according to the OED, is 'an essential or characteristic part of something abstract', so it *is* more than just people. However, these elements cannot just be anything that is associated with the organization; they have to establish policy, objectives and processes to achieve those objectives, perhaps directly or through interaction with other elements.
4. 'Establish' means 'to set up on a firm or permanent basis'. Accordingly, an XXX policy document would be part of the XXX management system as are top management and the XXX controls.

In conclusion, an XXX management system is:

everything that is associated with the organization that interacts to establish XXX policy, XXX objectives and XXX processes to achieve those objectives.

How management systems work

The continual improvement engine

Cyclic behaviour

The cyclic behaviour of a management system is illustrated in Figure 2 by direct reference to those clauses that contribute to that behaviour. The diagram can be regarded as a representation of a conceptual engine where repeated cycles have a tendency to render the management system self-healing (see below); and continually improve the suitability, adequacy and effectiveness of the management system.

There are various inputs into the continual improvement engine. The action of the engine is to turn these into actions. The results of these actions feed back into the engine via a feedback loop.

Inputs, outputs and the feedback loop

Some of these inputs correspond to identical core text requirements. These are:

1. performance measurement (Subclause 9.1);
2. internal audit (Subclause 9.2); and
3. management review (Subclause 9.3).

Subclauses 8.1 and 9.3 b) require an organization to respond to operational change, and thus operational change also provides an input into the continual improvement engine.

In practice, there may be other inputs. The first only applies if the organization opts for certification. In this case, the results of certification audits will provide additional inputs. The second applies to all management systems, regardless of whether they are certified or not, and that is the occurrence of an incident.

Subclause 10.1d) requires an organization to review the effectiveness of corrective action. For convenience, this has been associated in Figure 2 with the management review, which requires top management to consider a variety of topics, such as trends in audit results, during its management reviews.

Step 1 – Determine whether input is a nonconformity

For all inputs, apart from operational change, the organization must determine whether the input is a nonconformity. If it is not, or if the input results from an operational change then the organization must

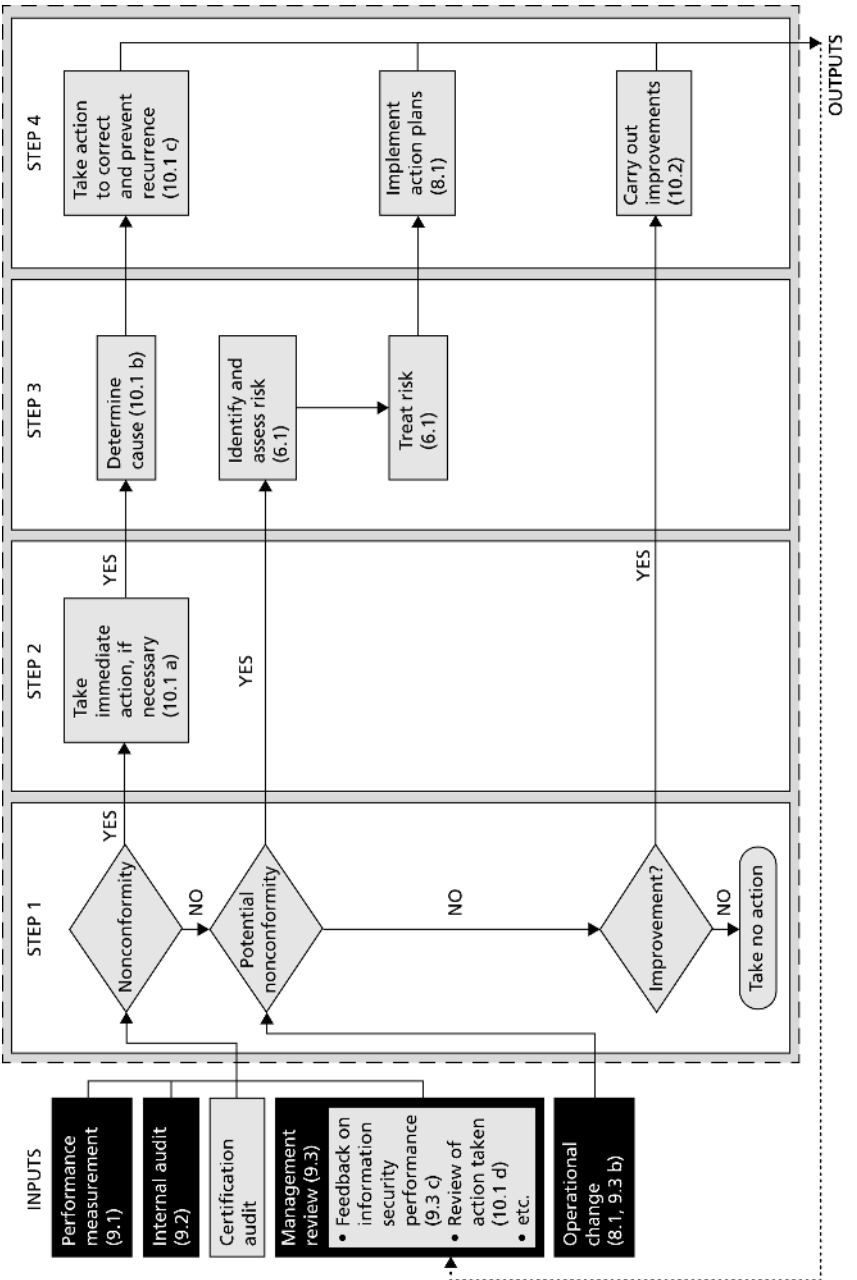

Figure 2: The continual improvement engine

determine whether the input is a potential nonconformity. If it is not, then it is either an improvement or no further action is required.

Step 2 – Take immediate action as necessary

If the input is a nonconformity, the requirements of Subclause 10.1a) require the organization to react to the nonconformity as applicable by taking action to control and correct the nonconformity and dealing with the consequences.

Step 3 – Plan considered action

If the input is a nonconformity, Subclause 10.1b) requires the organization to determine the cause of the nonconformity. The subclause also requires the organization to determine if similar nonconformities exist, or could potentially occur.

If it is a potential nonconformity then Annex SL regards it as a risk. The organization needs to identify and assess the risk as specified in Subclause 6.1 (see the section entitled 'Risks and opportunities' in Chapter 3). The organization then needs to decide what actions it wants to take to address these risks.

Note that potential nonconformities may be identified in Step 2 or as a by-product of the root cause analysis in Step 3.

Step 4 – Take considered action

If the input is a nonconformity, Subclause 10.1c) requires the organization to take action. The requirement is that the result shall eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere. The other actions are the implementation of the plans (Subclause 8.1) to implement the actions determined in Subclause 6.1 and carry out improvements (Subclause 10.2).

Nonconformities

Remarks about the definition

ISO defines 'nonconformity' as 'non-fulfilment of a requirement', where in turn ISO defines 'requirement' as a 'need or expectation that is stated, generally implied or obligatory'. A note to the definition states that 'generally implied' means that it is custom or common practice for the organization and interested parties that the need or expectation under

consideration is implied. Another note states that a 'specified requirement' is one that is stated, for example in documented information.

Example

On April 22, 2010, following an explosion two days earlier, a large drilling rig sank into the Gulf of Mexico, unleashing an unhealthy, toxic gush of oil that continued leaking from the stricken well for the following five months.

One of the most obvious nonconformities would have been the presence of oil on the surface of the ocean. In accordance with Subclause 10.1b), the oil company concerned took action to stem the flow of oil and clean up the pollution. In accordance with Subclause 10.1c), the company then sought a more permanent solution which involved pumping mud and cement into the well.

This example illustrates the need to contain and repair the damage caused by the nonconformity while seeking a more permanent solution.

Root causes

The root cause of a nonconformity is not always obvious. Because of this, the standard requires top management to consider trends in nonconformities and corrective actions (Subclause 9.3c)). Study of several apparently unrelated nonconformities may lead to the identification of common factors and hence the root cause. If at first view a nonconformity appears to be someone failing to follow a procedure, it could be because of poor training or the procedure could be impossible to follow in extenuating circumstances.

Documented information

With regards to Subclause 10.1, an organization is required to retain documented information as evidence regarding the nature of the nonconformities and any subsequent actions taken and the results of any corrective action.

There is no documented information requirement in Subclause 10.2. However, Subclause 9.3f) requires top management to consider opportunities for continual improvement in its management reviews.

Evidence of conformance to Subclause 10.2 ought therefore to be found in the required documented information for management reviews.

The documented information requirements for such other clauses are discussed in Chapter 3.

Understanding management system standards

General

In an ideal world, there are a variety of properties that a management system standard ought to possess. Real management system standards possess these properties to a greater or lesser extent; for example, ISO/IEC 27001:2013 satisfies all of them, whereas they are only partially satisfied by the preceding version (ISO/IEC 27001:2005).

These properties concern the order of implementation, conformance, self-healing properties, alternative requirements, impartiality, duplicate requirements and notes.

Requirements can be implemented in any order

In some sense, a management system is analogous to a reciprocating piston engine (for example, as used in a conventional motor car). The engine specification, as one might find in a sales brochure, dictates what the engine must look like and perform once it has been built. This type of specification does not prescribe how it is to be built. Likewise a management system standard dictates what the management system must look like and do, once it is operational. A management system standard does not specify how it should be built. Indeed, there are many ways in which a management system can be built – some better than others – as explained in Chapter 3. Thus one should conclude that the order in which requirements are presented in a management system standard should not be taken to imply the order in which they are to be implemented. ISO/IEC 27001:2013 makes this property absolutely explicit in Subclause 0.1 by stating 'The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purpose only.' The management system will work exactly as described in the previous section.

For conformance all requirements must be met simultaneously

Again using the analogy of the motor car engine, once built and started, all of the different processes of the management system will operate together in a relationship very much as described in the previous section. All requirements (permitted exclusions excepted) ought thereby to be seen to be met simultaneously.

This might appear to be a statement of the obvious, but it may affect one's interpretation of a management system standard. When reading a particular requirement do not assume that other requirements, particularly those that are presented later in the standard, have yet to be applied. In a motor car engine, when the piston travels downwards to suck in a fresh charge of combustible material, it has yet to travel up to ignite the mixture, but it did that on the previous cycle. A much safer assumption is that all requirements are met simultaneously.

A conformant management system is self-healing

Clause 10 contains requirements for taking action to identify and correct nonconformities. These have the effect of making the management system self-healing. It is as if as soon as part of the management system becomes nonconformant, the corrective action requirements spring into action to correct the nonconformity, thereby rendering the whole management system conformant once again. Viewed in this way the life of the management system is a sequence of conformity – nonconformity – corrective action – conformity and so on.

It does not matter if the organization knows about one or more nonconformity at the time of a certification audit, provided that it is dealing with it in accordance with the requirements of Clause 10. From a certification perspective, it is a good opportunity to see the corrective action component of the management system in action.

Alternative requirements

Take care when reading comma delineated lists. If the list ends with the word 'or' it means that the management system must conform to at least one item in the list (i.e. the use of the word 'or' should be interpreted as meaning 'and/or'). If it ends with the word 'and' it means that the management system must conform to every item in the list. For example:

1. Subclause 7.2 b) states 'ensure that these persons are competent on the basis of appropriate education, training, or experience'. This means that people shall be competent on the basis of appropriate education and/or training and/or experience. Thus someone might be competent on

the basis of education and training, while someone else might be competent simply on the basis of their experience; or

2. Subclause 9.3 states 'Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness'. If it transpires that the management system is no longer adequate then the management system would be nonconformant with this clause.

Impartiality

Standards written in conformance to Annex SL may at first view appear somewhat bland. This is because the intention is only to state *what shall* be done, not *how it might* be done. If the latter type of requirement does appear in a management system standard it forces all organizations to do it that way, and that may not be the best way for all organizations.

Duplicate requirements

Care has also been taken in Annex SL to ensure that requirements are only stated once. This is because there is a danger that duplicated requirements at best confuse and at worst contradict. It is now ISO practice, for example, to state the requirements for documented information within the clause, or group of clauses, to which it relates. For instance, Subclause 4.3 states the requirements for determining the scope of the management system. The final paragraph states 'The scope shall be available as documented information'. Thus the requirements for documented information are scattered throughout the standard. They ought not, however, be collated into one place as that would give rise to a duplication.

Notes

A note in an ISO management system is intended to assist readers to understand a requirement. It does not modify the requirement or imply that a particular way of meeting the requirement is itself a requirement. A sure test of one's understanding of a note is that the requirement should not change if the note was ignored.

Evolution of management system concepts

Early days

Perhaps the most well-known management system standard is ISO 9001. First published in 1987, it was based on British Standard BS 5750, itself first published in 1979. The standards did not specify *what* to manufacture but *how* the manufacturing process ought to be managed in order to ensure that the product, as delivered to the customer, met the customer's requirement. It was for this reason that they became known as management system standards.

These early standards were orientated towards procedures: a procedure for contract review, a procedure to control and verify product design, etc.

There was no concept of preventive action or continual improvement. There was nevertheless a concept of inspection and testing. This applied:

1. on receipt of components and other materials that would be used in the organization's product;
2. on product completion, prior to dispatch; and
3. during the process of design and manufacture, if required by the organization's quality plan.

From a conformance perspective, the emphasis was placed on conformance with procedures rather than the process of management. This had the unfortunate effect of divorcing quality from the management process and creating mountains of paperwork. Indeed one chief executive was heard to say, having appointed the quality manager, 'Your job is to get BS 5750, but don't bother me, I've got a business to run'!

Enter preventive action

The concept of preventive action was introduced in the 1994 revision of the standard. Effectively this invited organizations to look ahead and take action to prevent nonconformities from happening in the future. Although it would be some years before it was recognized as such, preventive action was effectively a risk assessment.

The emphasis of conformance with procedures, however, remained. Judging from comments made by quality assessors at the time, organizations were prone to creating the most marvellous procedures, as if having the best thought-out procedure was the key to a successful certification. Alas, such procedures, not being founded in reality, were often a cause for numerous nonconformities. Organizations would busy themselves immediately prior to a certification audit and, by endeavouring to ensure that the paper trail was complete, hoped to

escape from nonconformity. Following the audit, management practice would then relax. Such behaviour did not escape the attention of the certification bodies, who instructed their assessors to recommend that organizations simply wrote down what they actually did. Nevertheless, it was clearly time for a major overhaul.

Plan-Do-Check-Act and the process model

The major overhaul came in the 2000 revision of ISO 9001. The emphasis was now placed on the organization's business processes. Moreover, the concept of continual improvement was introduced, based on the Deming 'Plan-Do-Check-Act' Cycle, and a new subclause appeared devoted entirely to management commitment. These changes have certainly gone a long way towards making management systems an integral part of managing an organization. Indeed, the same chief executive quoted above personally oversaw the transition of his company's quality management system to ISO 9001:2000 and made absolutely certain that it directly supported his business.

Risks and opportunities – the depreciation of preventive action

The concept of risks and opportunities emerges with Annex SL and will feature in the next revision of ISO 9001 (anticipated in 2015). However, the concept of risk management has been practised by some organizations in their quality management systems for a long time. If an organization's products and services are varied, as is the case with a consultancy company for example, then it is unlikely that every product line or project will require exactly the same quality controls. The necessary controls are determined by risk assessment. One considers the product or service life cycle in its entirety and asks what can go wrong at each stage. Controls are then introduced to prevent the events that could lead to nonconformities, or at least detect them when they occur. In developing quality systems in this way, it was noticed by assessors that this practice is exactly equivalent to preventive action. Indeed, this case has been taken further by the authors of Annex SL who note:

> *This High Level Structure and Identical text does not include a clause giving specific requirements for "preventive action". This is because one of the key purposes of a formal management system is to act as a preventive tool. Consequently, the High Level Structure and Identical text require an assessment of the organization's "external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s)" in clause 4.1, and to*

> *"determine the risks and opportunities that need to be addressed to: assure the XXX management system can achieve its intended outcome(s); prevent, or reduce, undesired effects; achieve continual improvement." in clause 6.1. These two sets of requirements are considered to cover the concept of "preventive action", and also to take a wider view that looks at risks and opportunities.*

The notion of risk and opportunities arises because quality is not just about risk management: product improvements are also about exploiting opportunities.

Integrated management systems

Part of BSI's business case for the development of BS 7799-2:2002, the standard that became ISO/IEC 27001:2005, was that it should emulate the concepts to be found in ISO 9001:2000 to facilitate the development of integrated management systems. BSI argued that with the development of other management system standards such as ISO 14001 (on environmental management systems), organizations might not be interested as they could finish up with too many management systems. However, this might not be the case if organizations had a single, integrated management system that conformed to two or more management system standards. Thus the concept of an integrated management system was born.

In 2006, BSI published PAS 99, a publicly available specification for integrated management systems. This provided guidance on how to combine two or more management systems together to form an integrated whole. At about the same time, Brewer, Nash and List took a different approach. They first realized that there was a common aspect to management system standards – the Plan-Do-Check-Act cycle – and regarded that as the 'engine' that should drive systems of internal control, see Figure 3. Subsequently they devised an architecture for integrated management systems (see Figure 4) [a].

There is much in common between this architecture and Annex SL, the difference being that Brewer et al. had to interpret a standard in terms of their architecture before it could be integrated, whereas with Annex SL, management system standards are built to a common architectural design – the high level structure and identical core text.

In 2012, with the publication of Annex SL, PAS 99 was republished with the revised title of *Specification of common management system requirements as a framework for integration*.

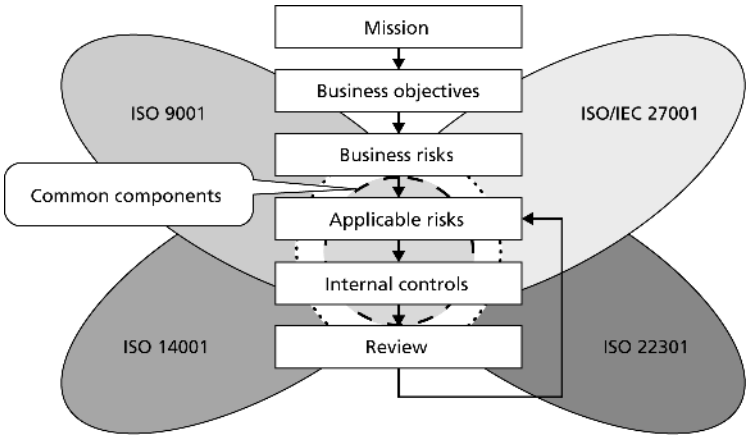

Figure 3: The common components of management system standards shown superimposed on the UK audit practices board's model of internal control

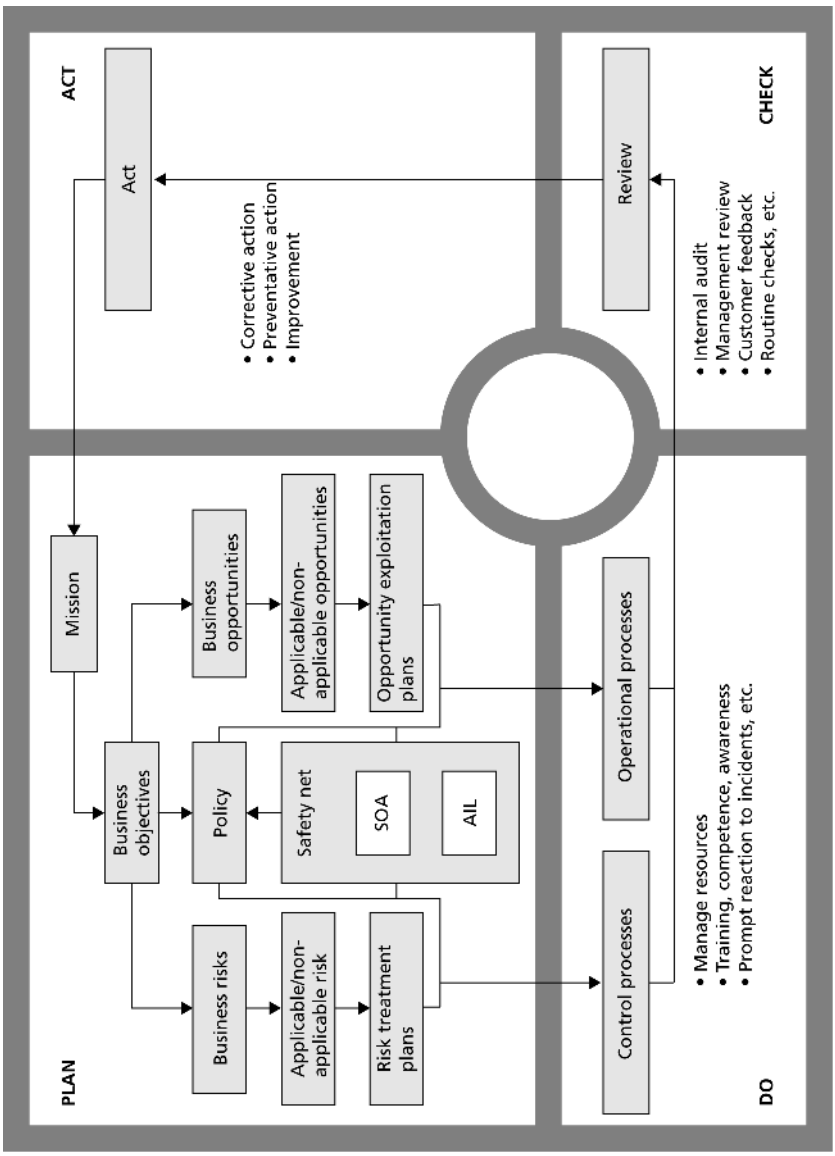

Figure 4: An architecture for integrated management systems

Chapter 3 – Understanding the new requirements

Introduction

The purpose of this chapter is to explain the Annex SL requirements and to provide guidance as to how these requirements can be met. The guidance is intended to be applicable to a wide range of differing management system implementations, appropriate to SMEs as well as much larger organizations. The chapter also provides advice to organizations that are building a management system for the first time.

The chapter is laid out as follows:

1. an explanation of what has happened to the PLAN-DO-CHECK-ACT (PDCA) concept;
2. a brief discussion of discipline-specific requirements;
3. an explanation of the identical core text requirements for all new and revised management system standards, together with implementation guidance:
    a) scope of the management system (Clause 4);
    b) policy and objectives (Subclauses 5.2 and 6.2);
    c) risks and opportunities (Subclause 6.1);
    d) operation (Clause 8);
    e) monitoring, measurement, analysis and evaluation (Subclause 9.1);
    f) audits and reviews (Subclauses 9.2 and 9.3); and
    g) management and support (Subclauses 5.1, 5.3 and Clause7); and
4. guidance on implementing a management system for the first time.

Note that an explanation of the Clause 10 requirements is given in Chapter 2 (in the section entitled 'how a management system works').

Whatever happened to PDCA?

ISO 9001:2000 introduced the concept of continual improvement and described it in the introduction to the standard using the Deming PLAN-DO-CHECK-ACT (PDCA) Cycle. Some other standards followed suit, but did so in a variety of ways. ISO 14001:2004 (on environmental management systems) cites PDCA in Clause 4 under the heading of

'Practical Guidance'. BS 25999-2:2007 (the forerunner of ISO 22301:2012 on business continuity), ISO/IEC 27001:2005 (about information security) and ISO/IEC 20000-1:2005 (regarding service management) all take PDCA a stage further, by adopting the model and building it into their requirement headings. In contrast, ISO 22000:2005 (on food safety management systems) does not mention it at all. However, Annex SL and standards such as ISO/IEC 27001:2013 do not mention PDCA. Organizations may therefore ask 'what has happened to PDCA?'

In looking at the above-mentioned standards, the extent to which guidance has been mixed up with requirements is quite noticeable. Unfortunately, a method for meeting a requirement might work very well for some organizations, but it may not work for all and for some it may even be a bureaucratic burden. It is therefore far better in a management system standard only to specify the *what* and stay clear of the *how*.

The requirement is for continual improvement of the management system. Specifically, Subclause 10.2 of Annex SL states 'The organization shall continually improve the suitability, adequacy and effectiveness of the XXX management system'.

The Deming Cycle is certainly an approach that organizations can take in meeting this requirement, but it is not the only approach: 6-Sigma, for example, is another. Certainly, the developers of ISO/IEC 27001:2013 had no wish to constrain organizations to use the PDCA model if they had a different approach to meeting the requirement for continual improvement. However, there were other reasons too as follows.

1. The PDCA concept does not just apply to the management system; it can be applied to anything. Thus an organization could design an awareness seminar (plan); run the seminar (do); analyse participant feedback (check); and determine how it could be improved (act). Because of this, the PDCA model was finding its way into supporting standards (e.g. ISO/IEC 27004:2009 on measurements) making them far more complicated than was necessary.
2. PLAN does not always follow ACT. One might plan a training course, but following review the only action needed to improve the course could be to modify the way in which it is delivered. This is a change to the DO. Thus in this case the cycle is PLAN-DO-CHECK-ACT-DO-CHECK-ACT etc. Indeed the improvement cycle is actually as illustrated in Figure 2, rather than as illustrated in Figure 5.
3. There is an implication that the first step in creating a management system is to implement the requirements associated with the PLAN phase of the PDCA model. However, as shown in the final section of this chapter, for an established organization, this is untrue. A better strategy is to start with the CHECK requirements and proceed in a manner that does not follow the cycle given in Figure 5 at all.

4. Subclause 4.1 of Annex SL was originally part of preventive action, which in all of the pre-2012 standards was part of ACT, not PLAN.

Nevertheless, there is still an association with the PDCA model in Annex SL. Writing down the major Annex SL subclause titles in their order of presentation counter clockwise in a circle (see Figure 5), suggests that PDCA has become 'ESTABLISH-IMPLEMENT-MAINTAIN-IMPROVE'. However, in answer to the question 'what has happened to PDCA?':

a) the *what* is 'continual improvement of the management system', whereas PDCA is a *how*; and
b) the cyclic behaviour of a management system is illustrated in Figure 2, not Figure 5.

Note that ISO 22301:2012 maintains the link with PDCA, just as in BS 25999-2:2007. Indeed from a technical perspective there is virtually no difference between the two standards. Effectively, ISO 22301:2012 is just an 'ISO version' of BS 25999-2:2007.

Discipline-specific requirements

The scope of this chapter is restricted to a discussion of the identical core text requirements and does not extend to a discussion of discipline-specific requirements. This is because, at the time of writing this book, there are too few examples of published management system standards that conform to Annex SL; two specific examples being ISO 22301:2012, *Business continuity management systems,* and ISO/IEC 27001:2013, *Information security management systems*.

Scope of the management system

Overview

There are four groups of requirements in Clause 4, arranged as shown in Figure 6. Subclauses 4.1 and 4.2 provide inputs to Subclause 4.3. They also provide inputs to Subclause 6.1.

Effectively, the purpose of the clause is to define the scope of the management system (Subclauses 4.1 to 4.3), and having done so, to require the organization to establish, implement, maintain and continually improve it, in accordance with the requirements of Subclause 4.4.

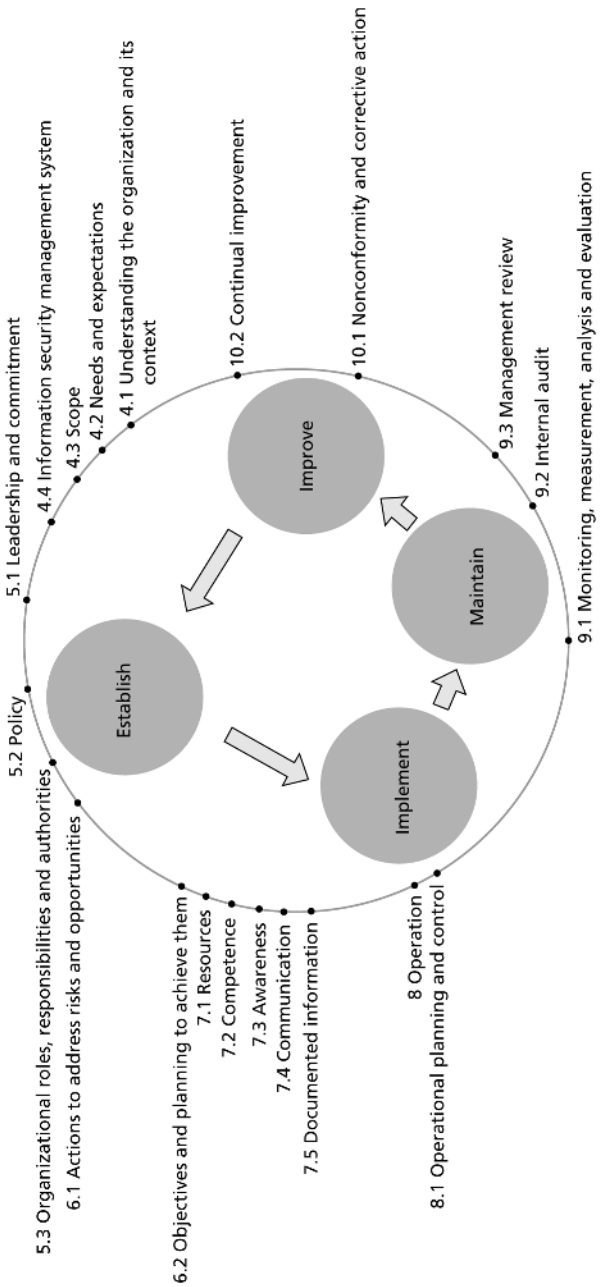

Figure 5: Annex SL management system requirements

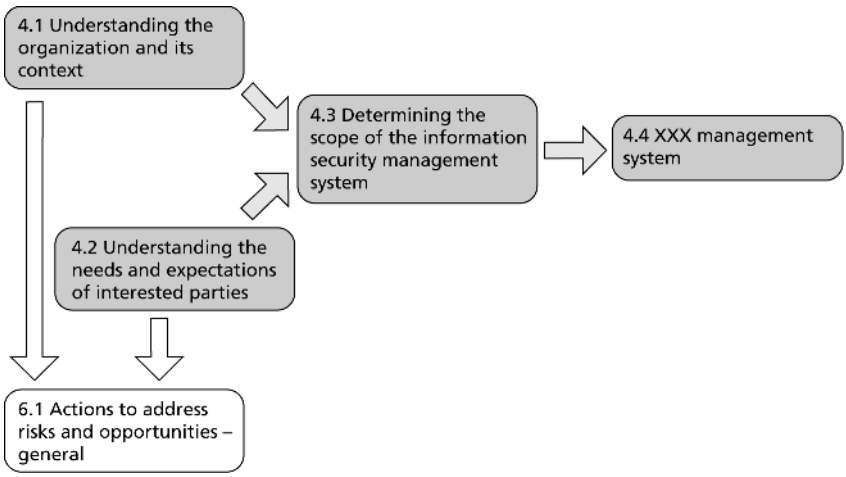

Figure 6: Relationship of requirements in Clause 4

Understanding the organization and its context

The requirement

There is a single requirement in Subclause 4.1, which states 'the organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its XXX management system'.

In accordance with the Oxford English Dictionary, an issue is an important topic or problem for debate or discussion. An organization's consideration of issues is not therefore confined to only a consideration of problems. It concerns all matters that could affect the well running of the management system and these may have a positive as well as a negative effect on the management system. Indeed, this is why the standard later (in Subclause 6.1) refers to risks and opportunities. As the management system belongs to the organization, it needs to fit in with the organization's way of doing things. First and foremost, it is there to help an organization achieve its objectives, not to hinder them. Understanding the organization and its context is therefore very important to the success of the management system.

Examples of issues include:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

- key drivers and trends that have an impact on the objectives of the organization;
- relationships with and perceptions and values of external [interested] parties;
- governance, organizational structure, roles and accountabilities;
- policies, objectives and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of the [members of the] organization and the organization's culture;
- information systems, information flows and decision-making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.[2]

The dynamic nature of issues

All issues are likely to change over time, albeit some, such as the social and cultural environments, more slowly than others. It is therefore prudent to maintain a watchful eye on such changes.

Relevancy

A good test for relevancy is to ask the following two questions.

1. Does the issue affect the ability of the management system to meet the requirements of the XXX management system standard?
2. Does the issue arise because of the management system and affect the ability of the organization to meet its objectives?

Understanding the needs and expectations of interested parties

The requirements

The requirements are that the 'organization shall determine:

a. interested parties that are relevant to the XXX management system; and
b. the requirements of these interested parties.'

(ISO/IEC Directives, Part 1, Subclause 4.2)

[2] ISO 31000:2009, *Risk management – Principles and guidelines*, Subclauses 5.3.2 and 5.3.3.

Interested parties

For many organizations, interested parties are likely to include past, existing and potential customers and past, existing and potential suppliers. For some organizations, regulatory authorities will also be interested parties. If the organization is part of a larger organization then those other parts may well need to be regarded as interested parties. Indeed an interesting case arises if one of them also has an XXX management system. In the case of an information security management system, if organization *A* (say) is responsible for general information security and organization *B* is responsible for application-level security, e.g. for the corporation's financial transactions, organization *A* may place constraints (e.g. in the form of policies) that organization *B* is obliged to meet. Thus, organization *B* does not have a totally free hand: organization *A* is an interested party and the constraints are organization *A*'s requirements.

The reference to past customers and suppliers is included because the organization may have surviving obligations such as guarantees and warranties even though they cease to buy or sell new products. Moreover, an organization ought to anticipate future needs, and hence the reference to potential customers and suppliers. There is little point, for example, in launching a new product or service if it fails to meet customer expectations.

Interested party requirements

Interested party requirements are likely to be documented in laws, regulations and contracts. However, by the ISO definition of requirement, a requirement can be a need or expectation that is generally implied. For example, a customer may well have an expectation that the organization will follow good information security practice, even though there might be no contractual obligation to do so.

Governance

Governance is about being a good steward, which according to the Oxford English Dictionary is 'a person employed to manage another's property'. In this case, the property is often money, which ultimately belongs to the company shareholders and creditors. In the wake of scandals resulting from unscrupulous behaviour in the boardroom, regulators and governments have stepped in and the notion of governance has been extended to taking care of the needs and expectations of all interested parties. There is thus a link between governance and Subclause 4.2. A cavalier organization that pays lip service to the discipline-specific requirements, hoping to gain certification on the grounds that what it does is acceptable to its top management,

ought to be ruled nonconformant with Subclause 4.2 if its actions are not consistent with the reasonable needs and expectations of interested parties.

Determining the scope

Scope

The Oxford English Dictionary defines the term scope as 'the extent of the area or subject matter that something deals with or to which it is relevant'. Thus the scope of a management system is 'the extent of the area or subject matter that is dealt with by the management system or which is relevant to the management system'.

It is important to realize that the scope of the management system is not the same thing as the scope of a certification audit and is generally far wider.

The requirement

The requirement in Subclause 4.3 states that in order to establish the scope of the XXX management system it shall determine 'the boundaries and applicability of the XXX management system'. The subclause also states that when 'determining the scope, the organization shall consider

— the external and internal issues referred to in 4.1, and
— the requirements referred to in 4.2.'

(ISO/IEC Directives, Part 1, Subclause 4.3)

Boundaries and applicability

The BSI Publicly Available Specification, PAS 99:2012, which concerns the integration of management systems, recommends that 'the organization should determine what the integrated management system is going to cover with respect to the specific disciplines (e.g. quality or information security) and their requirements and to the boundaries of operation'. Thus one may reasonably conclude that the phrase 'boundaries and applicability' is a reference to the extent of the organization's operational processes that are relevant to information security. For example, if people work from home, or the organization uses an internet service provider's servers to host an online catalogue then all of these are candidates for inclusion within the scope of the management system.

Choosing the boundaries wisely

Top management is the person or group of people who directs and controls the organization at the highest level. In accordance with Subclause 5.2, top management is responsible for establishing information security policy, and by Subclause 9.3 it is responsible for reviewing the management system. If there is any issue that prevents top management from conforming to such requirements, then it would be wise to redefine the organization to be a subset of its former self, as illustrated in Figure 7.

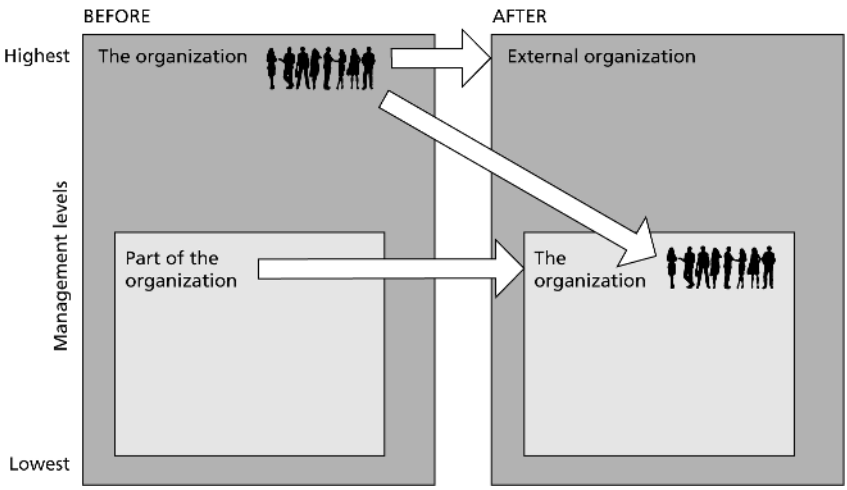

Figure 7: Redefinition of an organization

In this case, following redefinition, those parts of the original organization which are now excluded become an external organization and most likely an interested party too. Any issues associated with the redefinition would have to be identified in accordance with Subclause 4.1. Likewise, the requirements and expectations of that external organization would have to be identified in accordance with Subclause 4.2.

Identifying elements that are external to the organization

As an aid to identifying all entities that are external to the organization that ought to be included within the scope of the management system, consider the activities of relevance to the organization that are performed by other organizations. If there is a dependency or interface

to that activity, then it is likely that the activity ought to be included within the scope of the management system. For example, if the organization has a website for taking customer orders, then the website and the customer activity of using the website ought to be included within the scope of the management system.

There is a note to the definition of 'outsource' to this effect. It says 'an external organization is outside the scope of the management system, although the outsourced function or process is within the scope'.

XXX management system

Subclause 4.4 simply states that the 'organization shall establish, implement, maintain and continually improve an XXX management system, in accordance with the requirements of this International Standard'. In effect, this requirement is the ignition switch for the continual improvement engine. Conformance with this requirement implies conformance with all the other requirements and vice versa.

Documented information

The requirement is that 'the scope shall be available as documented information'. There is no requirement to document the organization's understanding of itself, its context, its interested parties or their requirements. However, there is also no requirement that prohibits an organization from doing that if it so wishes. For example, documented information concerning customer and supplier details and contractual requirements is likely to exist for the purposes of managing the business of the organization.

Policy and objectives

XXX policy

The requirement

Subclause 5.2 requires top management to 'establish a XXX policy that

— is appropriate to the purpose of the organization
— includes a framework for setting XXX objectives;
— includes a commitment to satisfy applicable requirements, and
— includes a commitment to continual improvement of the XXX management system'.

(ISO/IEC Directives, Part 1, Subclause 5.2)

Appropriateness

For the policy to be appropriate to the purpose of the organization it really ought to show how its objectives (see subsequent section) support the overall purpose of the organization and covers all of its functions. For example, if one of its purposes was the provision of 24x7 help-desk facilities to its customers, then high availability of its IT ought to be an objective.

Framework

Subclause 5.2c) requires the policy to contain a framework (e.g. a process) for setting the objectives.

Commitments

The wording of the standard implies a simple statement of commitment (e.g. 'Top management is committed to …') will suffice. However, top management ought perhaps to consider wording the policy to demonstrate their commitment rather than just merely stating that they are committed. Their commitment ought then to be self-evident from reading the policy. For example, the policy could reflect their understanding of the needs and expectations of interested parties and their direction to fulfil those needs through the realization of XXX measures that are fit for purpose and their enthusiasm for conformance to the XXX management system standard. The former demonstrates the commitment referred to in Subclause 5.2c) and the latter to the commitment referred to in Subclause 5.2d).

Documented information

Subclause 5.2e) requires the XXX policy to be available as documented information. Other subclauses require it to be communicated within the organization, and, as appropriate, to be made available to interested parties. The purpose of these subclauses is to ensure that those people and organizations who are obligated to comply with it, for example through employment or other contracts, know what it is. By making it, or parts of it, available to interested parties could also be used to support the organization's marketing activities.

As noted in Chapter 2, Annex SL does not give names to documented information, thus an organization is under no obligation to produce a document with the title 'XXX Policy'. However, if a certification auditor wanted to see the documented information concerning (or relating) to XXX policy, the organization ought to know where it is. Note the form of

words ('documented information concerning…'). A certification auditor ought not to be asking to see the XXX policy document.

XXX objectives

The requirement

Subclause 6.2 requires the organization to establish XXX objectives at relevant functions and levels. It then states that these 'objectives shall

— be consistent with the XXX policy
— be measurable (if practicable)
— take into account applicable XXX requirements
— be monitored
— be communicated, and
— be updated as appropriate'.

The subclause further requires that 'when planning how to achieve these objectives the organization shall determine

— what will be done
— what resources will be required
— who will be responsible
— when it will be completed
— how the results will be evaluated'.

(ISO/IEC Directives, Part 1, Subclause 6.2)

Functions and levels

The term 'function' in Subclause 6.2 refers to the functions of the organization. The term 'level' refers to the level of management of which top management is the highest. These interpretations derive directly from the ISO definitions of organization and top management (see Chapter 2).

As an example, at the highest level there would be XXX objectives that provide overall direction for the management system (e.g. 'To ensure business continuity in the event of significant incidents or disasters'). Such objectives are typical of those that top management might include in a business continuity or information security policy, and for this reason one might refer to them as policy objectives. At the next level, the various functions of the organization may well have specific XXX objectives. At the lowest level, XXX relevant actions may be placed on individuals, for example as an output of a meeting, and each of these will have an objective.

Note therefore that there can be a large number of objectives, which is why Subclause 5.2 requires a framework for setting objectives in the policy rather than the objectives themselves. It should be further noted, however, that there is nothing inconsistent in Subclause 6.2 with general management practice, and organizations ought to find that they comply with this requirement as a matter of course.

Types of objective

Broadly speaking there are two types of objective: those that set a general direction and those that set a quantifiable goal or target.

Objectives that set a general direction may not be measurable. There may, however, be evidence, e.g. through a lack of incidents, that the objective is being met. A case in question would be an objective to preserve the confidentiality of customer data. The loss of an unencrypted CD would indicate that confidentiality had not been preserved. However, one could not be certain unless the data reappeared on a website or newspaper. Such objectives may not be bounded in time. In such cases the requirement concerning 'when it will be completed' would not be applicable.

Those that set a quantifiable goal or target are in general measurable and would have a definite completion date.

Documented information

Subclause 6.2 requires the organization to retain documented information on the XXX objectives.

Risks and opportunities

Actions to address risks and opportunities

The requirement

Subclause 6.1 concerns actions to address risks and opportunities. Specific management system standards may have additional clauses, either in this section and/or in Clause 8 to deal with discipline-specific risk assessment requirements. For example ISO/IEC 27001:2013 has information risk assessment and related requirements in Subclauses 6.1.2, 6.1.3, 8.1 and 8.2, and ISO 22301:2012 has similar requirements in Subclauses 8.2 and 8.3.

Subclause 6.1 refers back to the issues determined in Subclause 4.1 and the requirements determined in Subclause 4.2, and requires the organization 'when planning for the XXX management system' to consider these issues and requirements to 'determine the risks and opportunities that need to be addressed to

— assure that the XXX management system can achieve its intended outcome(s)
— prevent, or reduce, undesired effects
— achieve continual improvement'.

It then states 'the organization shall plan

a) actions to address these risks and opportunities, and
b) how to
   — integrate and implement these actions into its information security management system processes
   — evaluate the effectiveness of these actions'.

(ISO/IEC Directives, Part 1, Subclause 6.1)

Why risks and opportunities?

The phrase 'risks and opportunities' was introduced into the identical core text because disciplines, such as quality, not only concern risk management, e.g. the avoidance of product recalls because of quality faults, but also of exploiting opportunities, e.g. delivering on market needs and customer satisfaction.

Documented information

There is no explicit requirement for documented information with regards to Subclause 6.1.

Operation

General remarks

Clause 8 consists of a single subclause: Subclause 8.1, entitled 'Operational planning and control', but as mentioned previously there may be other discipline-specific subclauses.

Subclause 8.1 has subclauses covering four topics. The first concerns planning, implementation and control; the second concerns documented information; the third, change management; and the fourth, outsourcing.

Planning, implementation and control

The organization is required to 'plan, implement and control the processes needed to meet requirements and to implement the actions determined in 6.1 by

— establishing criteria for the processes
— implementing control of the processes in accordance with the criteria'.

(ISO/IEC Directives, Part 1, Subclause 8.1)

The requirements are the requirements of the management system standard concerned and those identified in Subclause 4.2. Thus the processes referred to will include all management system processes, and all others that an organization determines as being necessary to meet XXX requirements.

The criteria of Subclause 8.1a) are used for the control of these processes. They could, for example, refer to when the process should start and finish; who authorizes it; or the scope or subject of the process.

Documented information

The organization is required to 'keep documented information to the extent necessary to have confidence that the processes have been carried out as planned'.

The answer to a question such as 'what evidence do I need to convince me that something has been done?' will act as a guide in determining how best to implement this requirement. However, in some cases there may be a need to convince other people, such as a court of law, and in these cases stronger and more factual evidence may be required. However, in all cases it is a question of risk: 'what if a process has not been carried out as planned, but I think it has?'; 'what actions would I take, and what would be the consequences if I am wrong?' The answers to these questions will also guide an organization to determine the extent of the documented information it requires. It should also be appreciated that the wording is an attempt to prevent the production of unnecessary documented information: management systems should not be bureaucratic paper-generating machines.

Change management

The organization is required to 'control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary'.

(ISO/IEC Directives, Part 1, Subclause 8.1)

The purpose of this requirement is to ensure that intended changes to the management system processes and XXX controls are properly controlled. The requirement recognizes that unintended changes may occur, perhaps as a side-effect of an intended change, or through error. In either case the consequence may be benign or it may have a detrimental effect on the management system or XXX performance. Thus, there is first a need to review the consequences, taking mitigating action as necessary.

Outsourcing

The organization is required to 'ensure that outsourced processes are determined and controlled'. These, of course, are processes within the scope of the management system.

Monitoring, measurement, analysis and evaluation

The requirement

Subclause 9.1 requires the organization to determine

— 'what needs to be monitored and measured
— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results
— when the monitoring and measuring shall be performed
— when the results from monitoring and measurement shall be analysed and evaluated'.

(ISO/IEC Directives, Part 1, Subclause 9.1)

Organizations are required to retain appropriate documented information as evidence of the results.

Finally there is a requirement to 'evaluate the XXX performance and the effectiveness of the XXX management system'.

This last requirement establishes the purpose of Subclause 9.1. Indeed, ISO/IEC 27001:2013 deviates from Annex SL by placing this requirement first. As a general recommendation, organizations ought not to monitor and measure for the sake of monitoring and measuring, or just because

they have the capability to do so. Instead, they ought first to decide what they want to know in order to evaluate the XXX performance and the effectiveness of the XXX management system, and work back from there to determine what to monitor and measure. By virtue of Subclause 6.2 this will include the monitoring of the progress in meeting the XXX objectives.

What is monitoring and measuring?

Monitoring is the determination of the status of a system, a process or an activity; whereas measuring is a process to determine a value. The status of something is the situation at a particular time during a process. Thus the difference is one of time, and with monitoring one is interested with how a value varies over time: for instance, is the number of virus attacks increasing or decreasing? Is the situation getting better or worse? Is an objective on target?

What to monitor and measure

XXX performance

The monitoring and measurement of XXX performance is discipline-specific, and as such is mostly outside the scope of this book. However, the organization will have established XXX objectives for various functions and levels (Subclause 6.2) and will also have established processes and possibly XXX controls (certainly for ISO/IEC 27001) in response to the discipline-specific requirements. An organization ought to monitor and measure the capabilities of these processes and controls during live operation.

All management system standards need to contend with nonconformities (Subclause 10.1). In addition, some need to contend with accidents, disruptions, emergencies, incidents and near misses. The occurrence of any of these affords an opportunity to make measurements on real events (rather than events deliberately manufactured by the organization to test their processes). In addition, monitoring of nonconformities, accidents, disruptions, emergencies, incidents and near misses allows an organization to determine whether it is under attack; whether incidents are on the rise, or decline; and whether near misses are harbingers of worse to come. However, these are not the only events that an organization could monitor. The technology that an organization might use in its XXX processes may monitor particular events, and an organization could include those in its list of what to monitor.

Candidates for measurement would be the XXX controls. A control is a means to reduce risk. Thus a quality control could, for example, be the

means to prevent the occurrence of a nonconformity. While measuring the effectiveness of some controls in isolation (e.g. the critical control points in food safety) may be a sensible course of action, for some disciplines, controls often work in concert where the failure of one control, say to detect a specification error at an early stage of product design, can be made up for any other at a later stage of design. In these cases, a better strategy would be to attempt to exercise groups of controls as a whole under simulated real-world conditions. How this is done and the types of measurements that would be made is, however, discipline-specific. For ISO 22301, such a mechanism – the business continuity exercise – is already built in as a requirement, together with an indication of the types of entities and their attributes, such as the actual time taken to recover to a particular level of service that an organization may wish to measure. For ISO/IEC 27001 the approach would be to simulate an information security attack and measure a variety of parameters, such as how much knowledge is required and how long it takes to defeat the controls. The idea here would be that if a person without any technical knowledge of IT, specialist equipment, insider knowledge of the security controls or inside help can defeat the organization's security within minutes, then one might conclude that the security plan, or at least part of it, is not very good. On the other hand, if the organization can withstand a sophisticated attack mounted by experts even with inside help over a period of months or years, then one might conclude that to all intents and purposes that aspect of security is unbreakable. Clearly care would need to be taken to ensure that such a simulation did not result in any undesirable consequences.

Effectiveness of the XXX management system

The most obvious candidates for monitoring are objectives and the occurrence of nonconformities. In addition, there will be other candidates depending on the processes that are within the scope of the management system. For example, at any one time, how many actions arising from review and other management system meetings are outstanding? If there is an IT help desk within scope, what is the status of the various trouble tickets?

Every activity associated with the management system and every management system process (e.g. risk assessment process) is a candidate for being monitored and measured. To assist with their identification, it is perhaps worth noting that there are several clauses that refer to the effectiveness of something:

1. XXX management (Subclause 5.1d));
2. the XXX management system (Subclauses 5.1f), 7.5.1b) and 9.3);
3. the implementation and maintenance of the XXX management system (Subclause 9.2b));

4. actions to address risks and opportunities (Subclause 6.1e) (second bullet point));
5. objectives (Subclause 6.2d));
6. actions to acquire the necessary competence (Subclause 7.2c));
7. awareness (Subclause 7.3b)); and
8. corrective action (Subclause 10.1d)).

As each of these is a requirement, then conformance needs to be demonstrated in some way. An organization could elect to do this by making measurements and using the results to evaluate the effectiveness. An organization is not obliged to take this approach, but it could be and therefore the activities and processes involved in meeting these requirements are candidates for measurement. Moreover, a number of clauses refer to the planning of something or to a something plan:

1. planning for the XXX management system (Subclauses 6.1 and 7.5.3);
2. planning the actions to address risks and opportunities (Subclause 6.1);
3. planning how to achieve its XXX objectives (Subclause 6.2);
4. planning the processes needed (and changes) (Subclause 8.1);
5. conduct internal audits at planned intervals (Subclause 9.2);
6. review the organization's XXX management system at planned intervals (Subclause 9.3); and
7. the audit programme (Subclause 9.2).

These are also candidates for measurement.

How to monitor and measure

The approach to making measurements

The making of measurements is a complete science in its own right. It is called metrology. A fundamental principle, however, is to start by determining the objective of the evaluation process. A metrologist would call this the 'information need'. It is the 'insight necessary to manage objectives, goals, risks and problems'.

One effectively works back through the analysis process to determine the measurements that one needs to make. Measurements are made of the characteristics or attributes of various entities. A metrologist would call these 'base measures'. Sometimes these base measures have to be combined to form what is known as a 'derived measure'. For example, most people are familiar with the car speedometer. This instrument measures the speed of the car, but in fact this is a derived measure. Depending upon design, what the instrument actually displays is the distance travelled in a fixed unit of time. Thus, distance and time are the base measures. The speedometer effectively calculates the speed by dividing the distance travelled by time.

Once all base measurements have been made and the derived measures have been calculated, the measurement process is complete and the analysis process can begin. The analysis would be performed in accordance with some algorithm or calculation of the organization's own invention. This will combine one or more base and/or derived measures with associated decision criteria. For example, if one was to make several measurements of the car's speed these could be plotted, during the analysis phase, as a graph of speed versus time. This graph would represent the car's acceleration. However, because the car might be travelling downhill against a strong headwind, further measurements could be made with the car travelling in the reverse direction, the hope being that the inaccuracies introduced by the gradient and headwind would be evened out. During the analysis a decision criterion could therefore be to use the average value of the speed measurements at a particular time after the car starts moving. The resultant graph is, of course, yet another measure. Metrologists give this a special name too and call it an 'indicator' which they define as a 'measure that provides an estimate or evaluation of specified attributes derived from a model with respect to defined information needs'.

The process of evaluation then proceeds by interpreting the indicator(s) in such a way as to address the information need. Such interpretation might differ depending on the information need. For example, if the objective was to support a review of the car for a magazine, the interpretation might result in descriptive text such as 'exhilarating', 'not as good as one might expect', 'great apart from a frustrating dead spot between 50 m.p.h. and 60 m.p.h.' However, if the car was being tuned for a race, the evaluation might be quite different, giving recommendations on how further adjustments might be made to improve performance.

Note that in order to satisfy a particular evaluation objective (i.e. information need) an organization might need to make many similar measurements over a relatively long period of time before starting the analysis and evaluation process. This is why the 'when the monitoring and measuring shall be performed' requirement is separate from the 'when the results … shall be analysed and evaluated' requirement.

The overall measurement, analysis and evaluation process is shown in Figure 8.

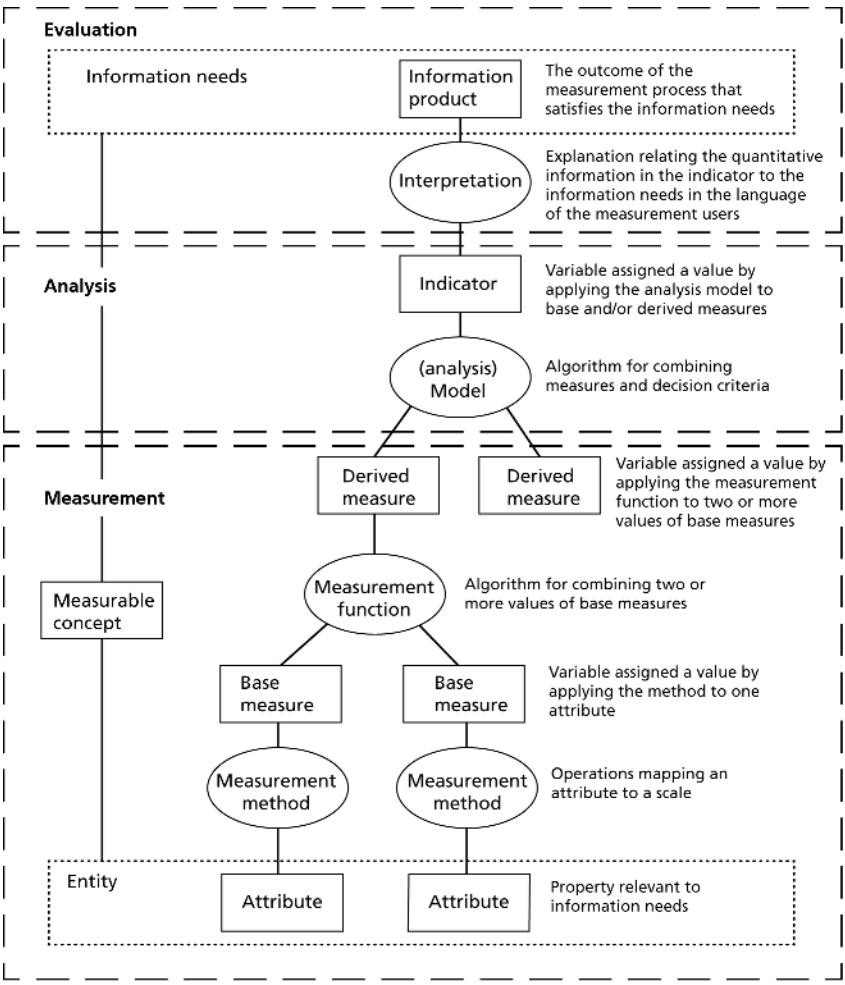

Figure 8: Schematic showing the relationship between the formal metrological term (information needs, etc.), as presented in ISO 15939:2007 and the requirement of Annex SL to monitor, measure, analyse and evaluate

Types of measure

Measures can be base measures, derived measures and indicators. However, there is another way to categorize measures and that is by the relationship of the information provided by the measure to the definition of effectiveness ('extent to which planned activities are realized and

planned results achieved'). Again there are three types:

1. implementation measures;
2. local effect measures; and
3. impact measures.

To explain these, it is useful to consider an example. Suppose that the concept of the management system is quite new to an organization. Upon reading Subclause 7.3, it decides that in the run-up towards certification it will put on an awareness seminar following the advice on subject material given later in this chapter. In this case, the organization's objective is simply to persuade as many people as possible in the organization to attend, and the planned result is say 95 per cent to allow for possible sickness and vacations. The requirement measurement is simply a head count. This is an **implementation measure**. It merely demonstrates progress in implementing an organization's XXX policies and procedures: if the target was 95 per cent – how many people actually attended?

Once the organization has achieved a high attendance rate, it might then look more towards the quality of the training. The plan might now be to set specific training objectives for the seminar and determine the extent to which the attendees have understood what they have learnt. In this case, the planned results, being an increase in awareness and understanding, are quite distinct from a mere head count. The measurements in this case may well involve an examination of the attendees. This type of measure is an example of a **local effect measure**.

Once the organization is confident that it can set realistic training goals and can meet them in practice, it might turn its attention to asking what impact does this have on the organization. The answer to this question lies in a change to the way the results are analysed as well as the need for additional measurements such as the number of incidents, near misses and nonconformities which are attributable to a lack of awareness. The indicator measures would now be examples of **impact measures**.

Note the progression from implementation measures through to impact measures. Organizations may wish to consider this as indicative of the level of experience it has with Subclause 9.1.

When to monitor and measure

As mentioned previously, organizations will have the opportunity to make measurements whenever there has been an accident, disruption, emergency, incident, near miss or a nonconformity. However, if there are none, or they happen infrequently, one perhaps does not really know

whether XXX controls will actually work as intended. It is therefore prudent to deliberately exercise them, as explained in the section on XXX performance above.

When to analyse and evaluate

Quite often, an organization might want to perform the analysis and evaluation as soon as the measurements have been made, but this rather depends on the nature of the measurements and the evaluation objective. For example, immediately prior to a management review (see below) an organization may wish to perform additional analyses, perhaps of the impact variety.

Measurement programme

Putting together the evaluation objectives, the whens and hows, will create a plan which may be referred to as a measurement programme. There is no explicit requirement in Annex SL to do this, but organizations might find such a plan to be useful as it will allow an organization to:

1. visualize any progression of measures, such as those in the example given in the section on types of measure;

2. ensure that those management system processes and aspects of XXX performance that it wishes to evaluate are incorporated into the plan; and

3. ensure that the dates for planned measurements and analyses have the proper relationship to other planned events, such as audits, management reviews and business continuity exercises.

Audits and reviews

Internal audits

Subclause 9.2 states: 'The organization shall conduct internal audits at planned intervals to provide information on whether the XXX management system;

a) conforms to
   — the organization's own requirements for its XXX management system
   — the requirements of this International Standard;
b) is effectively implemented and maintained'.

Subclause 9.2 continues by stating: 'The organization shall:

a) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
b) define the audit criteria and scope for each audit;
c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
d) ensure that the results of the audits are reported to relevant management, and
e) retain documented information as evidence of the audit programme(s) and the audit results'.

(ISO/IEC Directives, Part 1, Subclause 9.2)

Audit programme(s)

It is for each organization to decide what it wants to audit, how it wants to audit, how often and by whom. It needs to produce a plan. The standard refers to this as an audit programme, and an organization can have more than one such programme.

The extent of the audit programme will depend on a variety of factors such as:

1. the scope of the management system;
2. whether the organization is spread across many sites, and how similar they are in terms of information security controls; and
3. the complexity of XXX systems and technology within the scope and the nature of the technology that is used.

Depending upon the discipline, the audit programme may also depend upon factors such as how process failures affect the organization's exposure to XXX risk (e.g. information security risk for ISO/IEC 27001 and business continuity risk for ISO 22301) and risk of the occurrence of nonconformities. If the slightest failure results in an unacceptable exposure then that process may require greater attention than those where even the grossest failure may not have even the slightest effect on risk.

What an audit is and what an audit is not

An audit is an examination of an activity by an independent person to a specified objective. It is not the re-performance of the activity, an incident investigation or the provision of assistance in the development of processes and controls. Look for evidence of conformity. If there are

nonconformities they will be found, but auditing is not an adversarial pastime. It clearly states in Subclause 9.2 that the purpose of internal auditing is to provide evidence of conformity.

Substantive versus conformance audits

There are two basic styles of auditing. In a substantive audit, the auditor only looks at the results of the processing and applies a reasonable test. Unreasonable results indicate that there is a process failure. It does not necessarily indicate where the failure occurred, only that there is one, or more precisely that the results are anomalous and further investigation is required (usually by the auditee). In a conformance audit, it is adherence to the process or procedure that is audited. There is an underlying assumption that if the process or procedure is followed correctly then the results will be correct. This is, of course, not always a safe assumption. Nevertheless, if one is just trying to show that the management system conforms to the requirements of a given management system standard then a conformance audit is all that is really necessary. However, if the organization has some other audit objective in mind, for example, if it has a particular question regarding the appropriateness or accuracy of a process, then a substantive audit approach may be more appropriate.

Example

An example of substantive auditing is illustrated in the following true story. An experienced engineer produced several pages of mathematics, concerning the acoustic positioning of a moving target, and showed it to his manager. The manager flicked through the various pages, clearly not paying much attention to their content, but pausing for a few moments on the last page and said, 'there is an error in here, go away and fix it'. The engineer did so. He found the error, corrected it and re-presented the results to his manager. The manager did exactly the same as before: a quick flip through all the pages and pausing on the last page said, 'Yes, you seem to have fixed that one, but there is another; go away and fix that'. The engineer was now very frustrated. He said, 'Look, you haven't read this. I agree there was an error in the first version, but why do you think there is one in this version?' The manager replied, 'Simple. In the first version your final equation was dimensionally incorrect – the left-hand side was in units of metres, while the right-hand side was in units of time. In the second version, the equation was dimensionally correct, but when the target is at 90° to a microphone, the speed of sound becomes infinite, and we both know that is a physical impossibility.' In reviewing the engineer's work, the manager had applied a substantive audit technique. He did not pay much attention to the process that the engineer had used to reach his final equation, but instead applied a variety of reasonableness tests to the final equation, i.e. the output of the process.

Such techniques can be invaluable in auditing processes such as risk assessment and business impact assessment, as required by some management system standards.

Auditing processes

When auditing a process, if there is a written procedure then the auditor can read it, consider and ask questions on whether it is followed in practice. An important question to always ask is 'what if that doesn't work'. An alternative is to listen to an explanation of what people do. Write it down in the audit report. Other people in the organization may well have a view on it. Ask oneself questions such as: 'is the process complete, sensible, cost effective, does it cover everything, what if that

doesn't work and is there a better way?' Beware, however, of following the assumptions of the author of the process, thereby missing exactly the same things that they did.

Audit results

Be careful in documenting audit results to be objective. Document what was done in sufficient detail for someone who was not present at the audit to draw the same conclusions.

If a nonconformity has been found, state clearly what it is by reference to the precise clause in the management system standard or organizational requirement. Indicate how serious the nonconformity is. For example, if the nonconformity is indicative of a systemic failure of a management system process; or that as a result, the organization is exposed to unacceptable risk, is in breach of contract or is acting illegally, then the nonconformity perhaps ought to be regarded as a major nonconformity, as would indeed a certification auditor. If the nonconformity does not meet any such criterion, but is rather an oversight or temporary lapse of control, then the nonconformity might be regarded as being a minor nonconformity.

It is also customary to identify potential nonconformities and mark them as observations.

If something rather splendid has been discovered, record that fact in the audit report and say why it is so good. Some auditors mark these as positive observations, but a marking such as 'acclamation' may be more appropriate. It will act as an encouraging example to other members of the organization and may well indicate an opportunity for improvement. Indeed, do identify opportunities for improvement.

Management reviews

The requirement

Subclause 9.3 is in four parts.

The first part is about the frequency and objectives of the reviews. It states: 'Top management shall review the organization's XXX management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness'.

Part 2 elaborates on what must be considered during the review, stating: 'The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the XXX management;
c) information on the XXX performance, including trends in:
   — nonconformities and corrective actions
   — monitoring and measurement results, and
   — audit results;
d) opportunities for continual improvement'.

Part 3 specifies the outputs: 'The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the XXX management system'.

Part 4 concerns documented information: 'The organization shall retain documented information as evidence of the results of management reviews'.

(ISO/IEC Directives, Part 1, Subclause 9.3)

Frequency and objectives

The frequency of meetings is left for the organization to decide. In many respects the management review is analogous to action taken by a captain in sailing a ship. The review ought to have at its disposal all relevant information concerning the XXX performance of the organization and is able to take action to ensure continuing suitability, adequacy and effectiveness. Suitability will cover the primary purpose of the standard, should that be stated in its introduction and the XXX objectives that the organization will have defined at the highest level.

Frequency is therefore determined from the answer to a question such as 'how long can top management (i.e. the ship's captain) afford to be off the bridge?'

For some organizations the answer may lie in having several meetings, spread over the year, which collectively meet the requirements of Subclause 9.3. It is also often better to have many short meetings, each designed to last no longer than an hour than to have fewer longer meetings.

Review considerations

The first part of the requirement spells out that the subject of the review is the management system, and the implication here is that the policies, objectives and processes to achieve those objectives shall all be reviewed.

Note that the requirement to consider changes in external and internal issues can be very wide ranging. It will cover a plethora of topics such as changes in legislation, technology, the social and political climate, market

trends, organizational direction, objectives, performance and structure. Note also that the consideration of trends may feed into changes concerning Subclauses 4.1, 6.1 and 8.1 in order to ward off undesirable outcomes. It forms part of the feedback loop referred to in Figure 2. One would also expect top management to ensure that the management system remains compatible with the strategic direction of the organization.

Review outputs

The primary outputs are in actuality those as illustrated in Figure 2 and, in terms of the ship analogy, correspond to those adjustments necessary to maintain the ship on course (corrective action) or steer towards a more desirable destination (improvements).

Documented information

It would be usual for the documented information to be in the form of minutes. However, it is the content of those minutes that actually provides evidence of conformance.

1. The various considerations required by the second part of Subclause 9.3 will be seen to be regularly discussed.
2. Actions will be seen to have been executed promptly.
3. It will be evident that decisions will have been made regarding continual improvement opportunities and changes to the management system.

Management and support

Leadership and commitment

The requirement

Subclause 5.1 requires top management to 'demonstrate leadership and commitment with respect to the XXX management system by

— ensuring the XXX policy and XXX objectives are established and are compatible with the strategic direction of the organization
— ensuring the integration of the XXX management system requirements into the organization's business processes
— ensuring that the resources needed for the XXX management system are available
— communicating the importance of effective XXX management and conforming to the XXX management system requirements

— ensuring that the XXX management system achieves its intended outcome(s)
— directing and supporting persons to contribute to the effectiveness of the XXX management system
— promoting continual improvement
— supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility'.

(ISO/IEC Directives, Part 1, Subclause 5.1)

There is also a note which states that reference to 'business' should be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

Demonstrating leadership and commitment

Leadership and commitment will be evident in the manner in which top management conducts itself in relation to the management system. Internally, this will be most apparent in management review meetings and through its communications within the organization. Externally, it will be most apparent in the enthusiastic way it conducts itself in certification audits, regarding these, for example, as opportunities to show off its management system and to look for further opportunities for improvement. As such, certification audits ought to be events to look forward to.

Leadership implies being first – leading by example should be the motto. The XXX policy may affect people within the organization in different ways, but if top management complies with the XXX policy in respect of the parts that apply to them and demonstrate understanding and commitment to those other parts, then it is highly likely that subordinate members of the organization will act likewise. If there is something about the policy that top management does not like, for example it is rather bureaucratic, then top management must change it. After all, it is top management's policy.

Conformance with particular parts of Subclause 5.1 will also be evident in certain items of documented information. For example, it is likely that evidence in support of c) to h) will be found in the minutes of meetings. There may be issues associated with these items, but there will be evidence that such issues are being raised, discussion is taking place, decisions are being made and the issues are being resolved.

Organizational roles, responsibilities and authorities

Subclause 5.3 requires top management to 'ensure that the responsibilities and authorities for roles relevant to XXX are assigned and

communicated'. Specifically, it requires top management explicitly to 'assign the responsibility and authority for:

a) ensuring that the XXX management system conforms to the requirements of this International Standard: and
b) reporting on the performance of the XXX management system to top management'.

(ISO/IEC Directives, Part 1, Subclause 5.3)

The responsibilities of top management are defined in Clause 5 (Leadership) and Subclause 9.3 (Management review). Subclause 9.2c) requires the audit programme to include responsibilities. Thus, the standard explicitly identifies four roles that are relevant to all management systems. These roles concern conformance, reporting of performance, top management and auditing.

Resources

Subclause 7.1 states: 'The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the XXX management system'.

Simply expressed, this requirement covers all the resources needed by the management system.

Competence

The requirement

Subclause 7.2 states: 'The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its XXX performance, and
— ensure that these persons are competent on the basis of appropriate education, training, or experience;
— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken, and
— retain appropriate documented information as evidence of competence'.

(ISO/IEC Directives, Part 1, Subclause 7.2)

Note the use of the word 'or' in item b. This is the example of alternative requirements referred to in Chapter 2. It means that people shall be competent on the basis of appropriate education and/or training and/or experience.

As stated in a note in the standard: 'applicable actions may include, for example: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons'.

(ISO/IEC Directives, Part 1, Subclause 7.2)

Staff assessments and appraisals

The traditional method for meeting this requirement in most organizations is through a process of staff assessments or appraisals, and whatever method an organization currently employs ought to suffice for conformance to this requirement, particularly the explicit requirement for the retention of documented information.

The fact that this is a common management system requirement and that the majority of organizations will already have a conformant process underpins that there is nothing really discipline-specific about it apart from the skills that people may require. A good approach is to maintain a matrix of staff and skills, highlighting those skills that are necessary for a particular job function. The skills should be weighted and values agreed at each regular period of assessment for how competent that member of staff is for each skill related to their job function. This approach will not only serve as a convenient record of competence but provide an analysis of training needs and skill shortages.

Awareness

The requirement

Subclause 7.3 states: 'Persons doing work under the organization's control shall be aware of

— the XXX policy
— their contribution to the effectiveness of the XXX management system, including the benefits of improved XXX performance
— the implications of not conforming with the XXX management system requirements'.

(ISO/IEC Directives, Part 1, Subclause 7.3)

In addition to these requirements, an organization may wish to include other topics, such as:

1. XXX principles (e.g. quality principles, information security principles);
2. what can go wrong (e.g. as relevant: how product nonconformities can occur, how the environment can be damaged, how service

provision can fail, how food can be poisoned, how disasters can occur and how information systems can be attacked);
3. what can be done to prevent, detect and rectify such problems;
4. instructions on the use of discipline-specific solutions (e.g. quality controls) of particular relevance, for example because they are new or ones that people seem to be having difficulty with;
5. what to do in the case of an XXX incident, accident, etc.;
6. management decisions, audit findings, incidents, accidents and lessons that top management now wishes the organization to learn; and
7. the XXX management system.

Documented information

There is no explicit requirement for documented information.

Awareness programmes

There is no requirement for anything called an 'awareness programme'. The requirement is for creating awareness. How that is done is for the organization to decide. However, in some organizations an awareness programme might be appropriate.

An awareness programme would schedule various awareness events over a period of time, e.g. a year, each with its own subject and audience. This would be a good approach if the total audience was large and there were a large number of subjects to cover. Note, however, that dependent upon staff turnover, once staff awareness has reached a certain level the need for a programme of this nature will diminish, as everyone is essentially aware of everything that they need to be aware of. In this case, awareness shifts to induction courses for new staff and briefing seminars and other means of communications (see below) to maintain awareness as things change. Organizations should also be mindful of the following.

1. The approach needed to create awareness is likely to depend on a variety of factors associated with the people concerned such as their seniority, education and social background. Different awareness sessions may therefore be needed for different groups of people.
2. Approaches which involve audience participation and group exercises are often more effective than seminars.
3. If top management is aware then it is easier to create awareness at the lower levels.

Example

As an example, during the roll-out of information security management systems to a number of government ministries and departments, the consultants concerned had involved the ministry and department heads in the risk assessment and risk treatment processes. Indeed it was top management that personally performed the assessment and treatment of risk with the assistance of their senior staff and IT support personnel. One day, a department head invited one of the consultants into his office and proudly showed off his new safe. The senior civil servant explained that he was using the safe to lock away his confidential papers at night – no longer did he want to leave them out for people such as the cleaners to see. He had worked this out for himself. He had not been told to do it. It was a direct result of his involvement and his leadership in the assessment and treatment of his department's risks. The story of his new safe quickly spread throughout his department in a top-down manner. No one was going to be caught out. Speedily, they all equipped themselves with safes and immediately started following their boss's good example.

Awareness campaigns

There is no requirement for having 'awareness campaigns'. The requirement is for creating awareness. How that is done is for the organization to decide. However, once again, they may be appropriate for some organizations.

An awareness campaign seeks to create awareness of a particular issue, such as something new or something that is not working satisfactorily, over a short period of time. Successful campaigns have three stages:

1. an initial briefing, to tell everyone what the issue is and what should be done;
2. a period of reinforcement, where various methods are used to reinforce the message. For example, if the organization has control over people's screen saver it can use the screen saver as a reminder of the message. If the organization has internal monitors, then these could be used to repeatedly cycle through a short slide presentation. Throughout this period there is a need to determine how well awareness is being increased; and
3. feedback, at the end of the campaign, hopefully to congratulate everyone and act as a final reminder of what they have learnt.

Example

As an example, an organization wished to raise awareness of its policy of locking confidential documents away when not in use, particularly when staff went home at night. Accordingly, during the period of reinforcement in raising awareness of this policy, selected staff would regularly inspect the workplace (a large open plan office with over 100 staff) after work. Both offenders and people who had set a particularly good example were rewarded with a sticker. A green sticker meant a job well done; an orange meant a warning; and a red meant a visit to the top manager's office to explain themselves. There were a few red stickers at the beginning of the campaign, but news quickly spread that the boss was firmly behind this policy, a fact reinforced by his own array of green stickers. Over the following few weeks the number of orange stickers speedily reduced to zero while the number of green stickers increased. The campaign over, the boss remarked upon its success at the next departmental meeting, thanking everyone for their support.

Communication

Internal and external communications

Subclause 7.4 requires the organization to 'determine the need for internal and external communications relevant to the XXX management system'. Thus the standard recognizes that both internal and external communications are important. If the organization was part of a larger organization, for instance the organization was the drawing shop in a large company, external communications can mean communication with the Board of Directors and other departments, as well as customers and suppliers and other interested parties such as the families of employees and the press.

The requirement continues by saying 'including (a) on what to communicate …' and two others as discussed below.

On what to communicate

Organizations ought to consider both normal and abnormal conditions.

During normal conditions, communications can be used as the vehicle for creating discipline-specific awareness (see above), as well as news (e.g. successful certification audits) to bolster morale. Communications can also

be used to warn of potential problems (e.g. a risk of product nonconformity) and pending disruptions (e.g. that equipment will be offline for maintenance). Other topics could include meeting minutes, audit and incident (or accident) reports, and lessons to be learnt.

During abnormal conditions, topics would include advisories about disruptions, alternative working arrangements and coordinating business continuity activities.

Essentially the topics include everything that the organization wants people, both internal and external, to know and do that is relevant to its XXX interests.

When to communicate

Especially in abnormal conditions, timeliness is a key factor. However, there may be certain restrictions that can affect release, such as information that could affect share price, or a wish to release information only when the full facts are known.

With whom to communicate

Because of the awareness requirement (Subclause 7.3, see above), communication will be required with all persons doing work under the organization's control. It is appropriate to communicate with all interested parties. There may also be other people and organizations, not considered in Subclause 4.2 as being interested parties, with whom communication may be appropriate, for example in the event of a disaster. These include:

1. families of staff (e.g. to provide good news of their relative's safety);
2. emergency services; and
3. the Press.

If regular communication was entertained with law enforcement agencies, for example because of the nature of the organization's business the incidence of fraud was high, then it would be appropriate to include them as an interested party. Such agencies will invariably have requirements, for example, pertaining to the collection of evidence. An organization may also wish to entertain communication with the Press during normal operations as a vehicle for providing market assurance.

Other factors

In addition to the Annex SL requirements, organizations may also wish to consider who shall communicate and the processes by which communication shall be effected.

It is important to decide who will perform the communication and to ensure that they have the appropriate authority, competencies and knowledge. To do otherwise could lead to miscommunication and confusion.

Note that in large corporations, and similar, there might be an organization that is responsible for all internal and external communications. From the perspective of the management system, that organization might be an external organization. One would need to cooperate with them in order to meet the requirements of Subclause 7.4. Any difficulty here ought to be treated as an issue in response to Subclause 4.1.

A communication process describes the manner in which a message (i.e. the input to the process) is delivered to the intended audience (i.e. the output of the process). To be successful, it needs to deliver the right message in a clear and unambiguous way. The choice of medium will depend on the message and the intended audience, and indeed there is a wide range of mechanisms to choose from, including:

1. briefings, meetings, seminars and conferences;
2. letters, staff magazines, memos, emails, posters and web pages (internet and intranet);
3. short movies and film clips; and
4. telephone and text messaging, etc.

The use of a combination of methods may also be appropriate. For example, material presented in an awareness seminar could be reinforced with intranet articles, posters and videos on internal monitors.

Documented information

There is no explicit requirement for documented information in Annex SL. However, it will be inevitable that organizations will create whatever they need. If communication is effected through a presentation, for example, then the presentation material is, of course, documented information. Moreover, some management system standards may have discipline-specific requirements with regards to communications (e.g. ISO 22301).

Documented information

Overview of the requirement

Subclause 7.5 concerns documented information. It is split into three subclauses:

1. Subclause 7.5.1, which deals with the documented information that must be retained;
2. Subclause 7.5.2, which deals with creating and updating; and
3. Subclause 7.5.3, which deals with the control of documented information.

Documented information that must be retained

Subclause 7.5.1 states: 'The organization's XXX management system shall include

— documented information required by this International Standard
— documented information determined by the organization as being necessary for the effectiveness of the XXX management system'.

(ISO/IEC Directives, Part 1, Subclause 7.5.1)

Thus, an organization is free to determine what information it wishes to retain in addition to that required by the management system standard to which it chooses to conform.

Note the phrase 'management system shall include', which appreciates the role played by documented information in establishing policy, objectives and processes.

There is a note to the requirement which explains that the extent of documented information for an XXX management system can differ from one organization to another due to a variety of factors, such as the type and size of organization, and the competence of people. The list of factors included in the note is not exhaustive, but is intended to reinforce the principle that an organization ought to decide the extent of documented information for itself. As a guide, there is little point in producing documented information that no one will ever read, but great value in:

1. documenting clear, accurate and precise instructions in those cases where:
   a. an organization wishes many people to carry out an activity in a common way; and
   b. an activity is performed so infrequently that people find it difficult to remember how it was performed before; and
2. maintaining accurate records of performance.

Creating and updating

Subclause 7.5.2 states: 'When creating and updating documented information the organization shall ensure appropriate

— identification and description (e.g. a title, date, author, or reference number)
— format (e.g. language, software version, graphics) and media (e.g. paper, electronic)
— review and approval for suitability and adequacy'.

(ISO/IEC Directives, Part 1, Subclause 7.5.2)

Once again, organizations are free to decide how they wish to meet these requirements, and provided information is identifiable (bullet point a) and of known provenance (bullet point c) then almost anything goes. The word 'appropriate' is important. It means that conformance to the three bullet points should be suitable or proper for that item of documented information in the circumstances in which it is used. It also implies that different approaches can be used for different types of documented information.

Control of documented information

Subclause 7.5.3 is in three parts. There is also a note at the end of the subclause, pointing out that the term 'access', as used in the second part of the subclause, can mean read-only, read-write, etc.

The first part states that 'Documented information required by the XXX management system and by this International Standard shall be controlled to ensure

— it is available and suitable for use, where and when it is needed
— it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)'.

The second part states: 'For the control of documented information, the organization shall address the following activities, as applicable

— distribution, access, retrieval and use,
— storage and preservation, including the preservation of legibility
— control of changes (e.g. version control)
— retention and disposition'.

(ISO/IEC Directives, Part 1, Subclause 7.5.3)

The phrase 'as applicable' is noteworthy as the requirement for the preservation of legibility only applies to handwritten information (e.g. is it clear enough to read and does not fade over time). Moreover, control of changes does not normally apply to records (a witness statement being

retracted and replaced by another would, however, be a counter-example). The use of the term 'disposition' is also noteworthy. It covers the transfer of documented information to somewhere outside the scope of the management system (and thereby not under the control of the organization), such as the return of customer information to the customer at the end of a contract, as well as the deliberate destruction of documented information, for example on the expiry of its retention period. Note that some retention periods are specified in law, e.g. in the UK by the Companies Act, for company records, and the Data Protection Act, for personally identifiable information.

The third part states: 'Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled'.

(ISO/IEC Directives, Part 1, Subclause 7.5.3)

Documented information of external origin would include, for example, copies of ISO standards and books. They are not subject to quite the same requirements as documented information produced internally as the organization, for example, has no control over suitability or adequacy. However, an organization may wish to associate its own identifier with the information (such as a reference number in a library) and there may be a need to control distribution, for example, because of copyright restrictions.

If documented information is produced for the organization by an external organization (e.g. a consultant) and is subject to the organization's review and approval, then it should not be treated as being of external origin.

Implementation guidance

Build strategy

If the organization is a start-up company, it really does have a blank sheet of paper and building the management system in the order that the requirements are presented in the standard is not such a bad idea. However, if the organization has existed for a while, it will most probably already have some sort of system of management and something akin to whatever the discipline-specific requirements specify shall be in place. It will also most likely be doing many things in a sensible fashion, otherwise it would be changing the way it does things. This observation is key to developing an efficient and effective implementation strategy.

Rather than implement the requirements in the order they are presented in the standard, a better strategy is to pretend that the management

system actually exists, and then use the self-healing properties (Clause 9 and 10) to turn it into one that really does conform to the standard.

The first step is to set up at least an embryonic management structure with which to manage the project. The next step is to recognize that although the diagram given earlier in Chapter 3 appears to start with ESTABLISH, and proceed to IMPLEMENT, MAINTAIN and IMPROVE, the best place to start is with MAINTAIN. Use the performance evaluation requirements (Clause 9 – measurement, audit and review) to discover what the organization already has in place in terms of the discipline-specific requirements and management system processes. A consultant might call this a gap analysis, but there is one big difference: one is actually making use of the Clause 9 management system processes to perform the analysis, and rather than then write up a report of gaps, one uses the requirements of Clause 10 to take immediate action. Thus, if one discovers a nonconformity, one takes immediate action to correct it, but if it is just something that would be 'nice-to-have', e.g. a better way of doing something, treat it as an improvement. It is not necessary to complete improvements before certification, however, if a pre-certification completion date has been set for the improvement, it clearly ought to be complete by the time of certification.

If certain discipline-specific requirements are met, e.g. there are quality (ISO 9001) or information security (ISO/IEC 27001) controls or a business continuity plan (ISO 22301) in place, one might get a head start on meeting the other discipline-specific requirements by reverse engineering. In this case, if there is a logical order to the way the discipline-specific requirements are presented in the standard, then one that investigates conformance to the requirements in the reverse order of presentation is the better way to proceed. This certainly should work for ISO/IEC 27001 and ISO 22301.

Awareness training and training in other skills that the organization deems relevant (see, for example, the discussion above on roles in the section on management and support) can start as soon as sufficient documented information has been put in place. For example, training of internal auditors cannot really be started until there is an agreed audit programme and audit procedure. Note that in this case, in addition to classroom training, trainee auditors may be given on-the-job training, performing audits which will kick-start the audit programme and build up a useful portfolio of audit reports.

In summary, one starts putting the management processes in place from day one. Record keeping starts from day one. One does not start at the beginning of the standard and implement the requirements in the order presented. Rather one starts in the middle and works towards the end and the beginning simultaneously, recognizing that Clauses 9 and 10 (see Chapter 2) are effectively the engine that drives and continually improves

the management system. Thus, even while the management system is being established, these clauses will be exercised many times over.

Preparation and project planning

Overview

Figure 9 shows a schematic of a project plan, which is based on over 10 years of experience in building and using management systems. The diagram shows two distinct regions of activity, called build and use. These words have been chosen to avoid confusion with the words used in the standard, which are establish, implement, maintain and improve. In particular, while the management system is being built, the organization will in fact be carrying out activities in conformance with *all* the requirements of the standard. The same is true when the management system is in use.

The diagram also shows the relation of build and use to various certification activities, namely the initial certification audit (which is in two parts) and the first surveillance audit.

Five milestones have been identified:

M1: Project start-up;
M2: Specifications approved;
M3: Ready for certification;
M4: Recommended for certification; and
M5: Fully operational.

M1 Project start-up

Project start-up will include all the activities normally required by the organization at the start of a project. However, at, or soon after, the start-up there ought to be at least a working definition of the organization, its top management and the scope of the management system.

One of the first activities ought to be the construction of a repository (#1, in Figure 9) for the documented information. This should be designed in such a manner that it is easy to demonstrate conformance with all the requirements of the standard. In that manner, the project team can ensure that nothing has been missed out.

As the project proceeds, documented information (#2) will be placed into the repository; and the management system processes will be created and put into operation (#3). The previous section suggests an order for doing this.

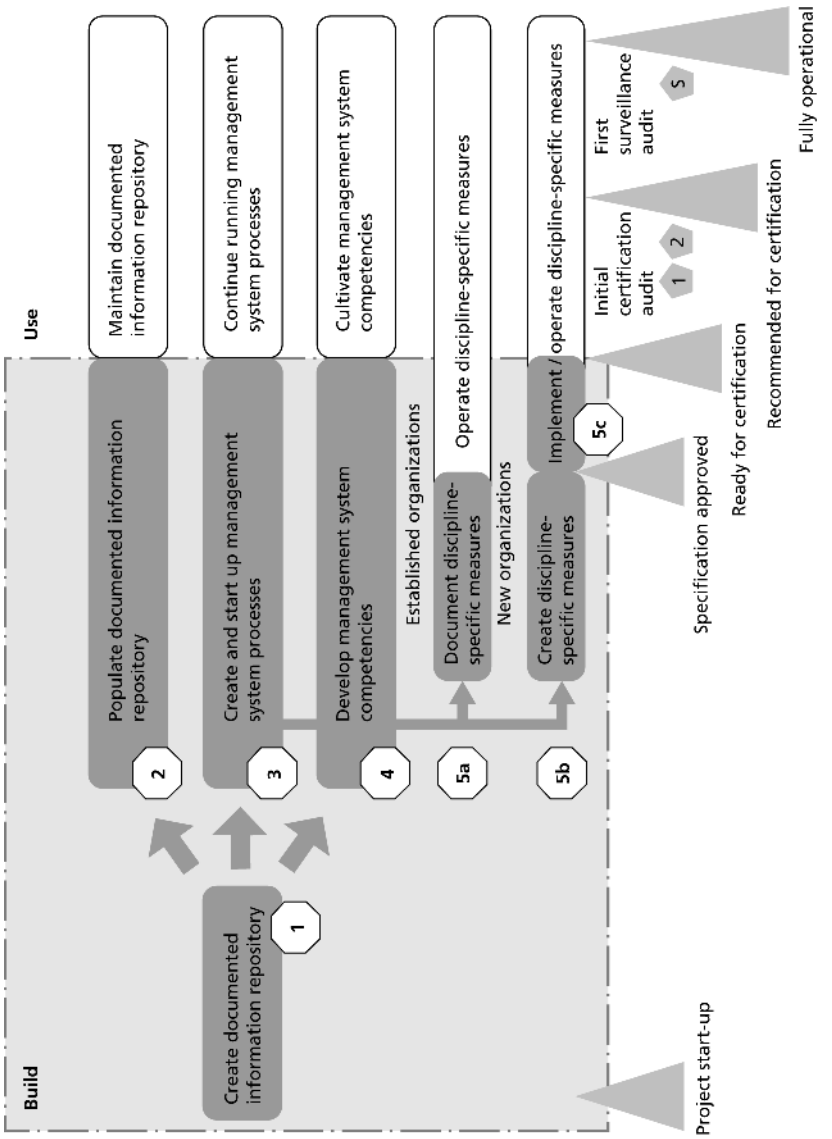

Figure 9: Schematic of a project plan

A management system is as much about what people do as the documented information that it amasses. Therefore, there is a need to ensure that the people involved with the management system (top management, internal auditors, etc.) have the necessary competence. How this is done depends on the competencies already possessed, but in cases where having a management system is new, the development of competencies (#4) is likely to proceed via a number of briefing sessions and training courses. Ideally training should be aligned to the organization, its objectives and policies. This will allow classroom training to be immediately followed by a period of on-the-job training, where the newly trained individuals can be put to good use in helping to build the management system. For example, the organization's audit procedures and audit programme (or at least preliminary versions of them) ought to be drawn up before internal audit training is commenced. A possible training course would then include:

1. explanation of the project, progress to date, and what will happen next;
2. audit theory and technique, explained in the context of the organization and objectives;
3. the audit requirements in the management system standard;
4. specific instruction and practice in the conduct of the organization's audit procedures; and
5. explanation of the audit programme and expectations from on-the-job training.

Immediately after classroom training the newly trained auditors would then practise their skills in carrying out the audit programme. For a period of time, however, this would be regarded as on-the-job training, and would therefore attract much closer supervision from an experienced auditor. If changes are required to the audit procedures or audit programme, then these would be administered in accordance with Clause 10 of the standard (i.e. they would either be regarded as improvements or actions to correct nonconformities).

With regards to the discipline-specific requirements, there are two cases depending on whether the organization is an established organization or is a new organization. In the case of an established organization, it will have discipline-specific matters in place, but these might not conform to the requirements of the standard or even be written down. The task (#5a) is therefore to document it and deal with nonconformities. If there is nothing at all, the task (#5b) is to create the discipline-specific matters and (#5c) to implement them.

M2 Specifications approved

Once all the specification-type documented information requirements have been met, top management can approve the management system

specification and confirm that milestone M2 has been achieved. At this stage, the documented information ought to pass a stage 1 audit. If the organization wanted a second opinion on how well it was doing, it would now be appropriate for a certification body to conduct a pre-assessment visit.

M3 Ready for certification

Once all the training (classroom and on-the-job) has been performed, and all the management system processes are up and running, top management ought to be able to pronounce that the management system is ready for certification (i.e. that Milestone M3 has been reached). There should be a wealth of documented information of the 'records of performance' variety to support this.

Note that if a certification body is asked to conduct a pre-assessment visit it should be done at the previous milestone, not here. At this advanced stage, the certification body ought really to be doing the initial audit.

M4 Recommended for certification

On completion of the stage 2 audit, the assessment team will produce its audit report and recommendation for certification, which should prove in favour of certification. The certification body will make its decision on the basis of the audit report and other information provided to it by the assessment team in accordance with its procedures. It would be unusual for the certification body not to uphold the assessment team's recommendation.

M5 Fully operational

Every six or twelve months the certification body will conduct a surveillance audit (also known as a continual assessment visit, or CAV), and every three years there is a reassessment audit, which is somewhat akin to the stage 2 initial audit in terms of coverage. However, the first surveillance audit is somewhat of a special occasion as it is a true test that the management system is indeed functioning as specified in the management system standard and has not, for whatever reason, lapsed into a state of doing nothingness immediately following certification. A final project milestone, milestone M5, is therefore associated with a successful first surveillance audit. From the perspective of the organization, a successful audit ought to be one where no major nonconformities are found.

Choice of documentation media

When deciding the form and storage medium for documented information there are four factors that ought to be considered:

1. where to store the information;
2. how to navigate it;
3. whether it ought to be static or dynamic; and
4. whether to duplicate or not.

If documented information is kept in the form of paper documents, one has to consider the requirements concerning its availability and suitability (e.g. is it the correct version) for use, where and when it is needed (Subclause 7.5.3). This is less of a problem if the documented information is maintained in electronic form and accessed through the organization's intranet or extranet, or even stored in a private or public cloud.

The ability to navigate by hyperlink has clear advantages, and is supported by many document formats including PDF, HTML and Word. One organization, which maintains its documented information in HTML on its intranet,[b] reported in 2004: 'In the space of a few minutes I had demonstrated how our management system had met about 50 % of the BS 7799-2 requirements'. Using hyperlinks, information is literally one or two clicks away. It speeds up management reviews and external audits considerably.

If the information, at least some of it, is stored in a database then it can be processed immediately prior to being displayed to the user. This has advantages in being able to display up-to-date information, such as monitoring and measurement results.

Finally, there is the question of duplication. An organization may well have copious documented information stored outside of the management system repository. It is best not to duplicate these, but instead refer out (link) to the current versions. References (or links) should be set up so that if the version changes, the reference (or link) does not.

Chapter 4 – Transitioning to the new management system standards

Introduction

The objective of this chapter is to provide guidance on how to transition an existing management system to a new version of a management system standard that conforms to Annex SL. The guidance only concerns the identical core text and does not address discipline-specific requirements. The guidance has been developed for standards that closely follow the ISO 9001:2008 requirements that led to the development of Annex SL. These standards include ISO/IEC 27001:2005 and ISO 22301:2012.

This chapter is laid out as follows:

1. Transition strategies;
2. Integrated management system considerations;
3. Areas requiring little or no change;
4. Areas that potentially require a rethink;
5. New requirements likely to be satisfied already;
6. New requirements that may present a challenge;
7. Areas where an organization may take the opportunity to improve; and
8. Summary.

Transition strategies

At first view the changes may seem significant. However, on the basis of experience it has been found possible to transition a management system quite quickly, e.g. within a few weeks. However, while doing so, opportunities for overall improvement were identified. Thus, there are two basic transition strategies:

1. a straightforward 'make-over', making the minimum necessary changes to the existing management system processes and existing documentation; or
2. take a completely fresh look at the management system, taking advantage of the revised standard to make, in the case of some organizations perhaps quite significant, improvements.

In both cases, it will help greatly if there is a detailed explanation of how the existing management system conforms to the non-Annex SL conformant standard(s). In particular, cross-references to the individual requirements by paragraph, sentence, bullet point and even phrase to the exact point in existing documented information will be found to be the greatest benefit. If such an explanation does not exist, then a good place to start would be to produce it. It is recommended that any explanation of conformance to the revised standard is produced with the same level of precision.

Integrated management system considerations

The issue

As discussed in Chapter 2, Annex SL uses the term *documented information* rather than the original terminology of *documents* and *records*, and depreciates the term *preventive action*.

However, transitioning an integrated management system to a standard that conforms to Annex SL must be done in a manner that preserves conformance to standards which are not Annex SL conformant. This means that the transitioned integrated management system must conform to conflicting requirements:

1. a requirement for having *documents* and *records* (in a non-Annex SL conformant management system standard) and a requirement for having *documented information* (in an Annex SL conformant management system standard); and
2. a requirement for *having* preventive action (non-Annex SL conformant standard) and a requirement for *not having* preventive action (Annex SL conformant standard).

Documented information

Chapter 2 explains the relationship between *documents*, *records* and *documented information* in terms of specifications and records of performance. It is important to realize that an organization does not have to call something by exactly the same name as it is referred to in a standard, provided the organization knows how it satisfies the requirements of each standard in question. Thus a solution would be to:

1. update all integrated management system documentation to use the Annex SL terminology (e.g. 'documented information' in this case);
2. state (somewhere in the integrated management system documentation, e.g. where conformance to a non-Annex SL

conformant standard is being discussed) that there are two types of documented information, Type S and Type P as defined in Chapter 2;.

3. refer to documented information of Type S or Type P as appropriate if a distinction is being made between documents and records.

The reason for recommending that existing management system documentation is updated to use the Annex SL terminology is because ultimately all management system standards will use that terminology.

Preventive action

While Annex SL does not use the term 'preventive action', there is an Annex SL requirement (10.1b) that refers to potential nonconformities), which states '… determining if similar nonconformities exist, or could potentially occur'. Thus it is the term *preventive action* that is depreciated, not the concept of potential nonconformities.

Requirement 10.1b) also states '… reviewing the nonconformity'. In conforming with this requirement, upon discovery of a nonconformity, an organization would review that nonconformity. As part of that review the organization would determine whether there were any associated potential nonconformities. In non-Annex SL conformant standards, the process may well then continue by producing a 'Preventive Action Plan', as illustrated in Figure 10. The existence of this plan is effectively outlawed by Annex SL, compelling one to identify its replacement. To do this, one simply needs to change the name. It could simply be referred to as an action plan, as illustrated in Figure 11.

Figure 10: Fragment of the preventive action process in a non-Annex SL conformant standard

Thus, transitioning to an Annex SL conformant standard would be replaced by a process of the form:

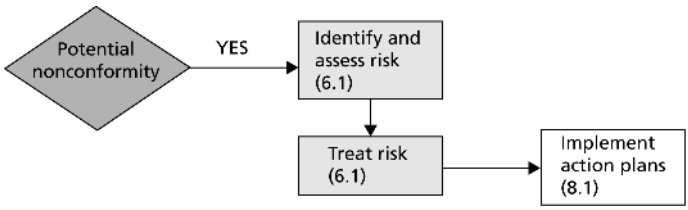

Figure 11: Replacement fragment in an Annex SL conformant standard

In explaining this process, in order to preserve conformance with non-Annex SL conformant standards, it will however be necessary to explain that:

1. 'identify risk' in the transitioned integrated management system satisfies any non-Annex SL conformant requirement for 'determining potential nonconformities and their causes'; and
2. 'treat risk' and 'implement action plans' in the transitioned integrated management system satisfies any non-Annex SL conformant requirement to 'determine and implement action needed'.

In addition, existing procedures may need to be augmented to react to nonconformities and take action, as applicable, to control and correct the nonconformity and deal with the consequences. Augmentation may also be required to determine whether similar nonconformities exist, or could potentially occur and to ensure that corrective actions are appropriate to the effects of the nonconformities encountered. It is possible that procedures already exist for these requirements, but under the heading of preventive rather than corrective action.

In addition, existing procedures may need to be augmented to react to nonconformities and take action, as applicable, to control and correct the nonconformity and deal with the consequences. Augmentation may also be required to determine whether similar nonconformities exist, or could potentially occur and to ensure that corrective actions are appropriate to the effects of the nonconformities encountered. It is possible that procedures already exist for these requirements, but under the heading of preventive rather than corrective action.

Areas requiring little or no change

Requirement changes

For people familiar with pre-Annex SL standards there are identical core text requirements that might either look quite alien or lack content. Indeed, the word 'generic' is a criticism that has been spoken against Annex SL. However, this is because of the desire to define *what* not *how*. To give an example, ISO/IEC 27001:2005 has a (discipline-specific) requirement to identify information security risks. The requirement continues by specifying in sub-bullets: identify assets, identify risks and identify vulnerabilities. The sub-bullets describe just one way to identify risks. There are other methods for identifying risk that do not do it that way. Thus the 2005 version of ISO/IEC 27001 states *what*: i.e. identify information security risks, and then proceeds to specify *how*: i.e. identify assets, identify risks and identify vulnerabilities. The 2013 version of ISO/IEC 27001 just states identify information security risks, i.e. the *what*. There is no mention of *how*. Indeed the terms assets, threats and vulnerabilities appear nowhere in the standard as a requirement or even as a note.

In this case, an information security management system that conforms to the risk identification requirements of ISO/IEC 27001:2005 must also conform to those of ISO/IEC 27001:2013. The fact that the identification of assets, threats and vulnerabilities is no longer a requirement is irrelevant. For this reason, there are quite a number of areas where an existing management system requires little or no change in order to conform to the corresponding Annex SL requirements. These areas are identified and discussed in the following subsections.

Policy

In the case of some pre-Annex SL management system standards there is a requirement to produce an XXX management system policy as opposed to what is required by Annex SL, which is just an XXX policy. Indeed, ISO/IEC 27001:2005, for example, goes as far as saying that the XXX management system policy is a superset of the XXX policy (where in this case, XXX = information security). The Annex SL requirement only to produce an XXX policy may cause confusion. 'What happens to the extra policy material that went into the management system component of the XXX management system policy?' is a question that some organizations might ask.

The answer is actually quite simple. The names that an organization wants to give to the various parts of its suite of documented information is not mandated by Annex SL. If an organization has a document or web page called 'ABC policy' that contained all the policy information

required by the pre-Annex SL version of the management system standards with which it claims conformance, then nothing needs to change provided:

a. there is a requirement to retain such information; or
b. the organization considers that it is 'necessary for the effectiveness of the XXX management system'; and
c. there are no additional discipline-specific requirements for documented policy information.

However, organizations may feel the need to explicitly add statements of intent in regards to Subclause 5.3, third and fourth bullets, and add further policy statements, for example, regarding external and internal communications. Indeed, a policy statement is often a convenient way to document conformance with a requirement.

Control of documentation

No changes ought to be required to existing documented procedures concerning control of documentation although minor adjustments may be required to the explanation of conformance. However, organizations should check for new discipline-specific requirements and deviations.

Management review

No changes ought to be required to existing documented procedures concerning management review, apart from ensuring that the topics listed in Subclauses 9.3a) to f) are considered. Minor adjustments may be required to the explanation of conformance. However, organizations should check for new discipline-specific requirements and deviations.

Internal audit

No changes ought to be required to existing documented procedures concerning internal audit although minor adjustments may be required to the explanation of conformance. However, organizations should check for new discipline-specific requirements and deviations.

Terms of reference for top management

A change may be required to accommodate the specific responsibilities given in Subclauses 5.1a) to h).

Responsibilities

A change may be required to accommodate the specific responsibilities given in Subclauses 5.3a) and b).

Awareness

A change may be required to accommodate the requirements of Subclause 7.4 as the process of creating awareness may be regarded as a form of communication.

Improvement

Ensure that existing procedures for continual improvement are extended to cover the suitability and adequacy of the management system as well as its effectiveness.

Areas that potentially require a rethink

Nature of challenges

There are two areas where the Annex SL requirements are not new to management system standards, but the way they are expressed may cause organizations to rethink their approach to conformance. The first concerns the scope of the management system and the second the XXX objectives.

Scope of the management system

During the course of revising ISO/IEC 27001, it became evident that there has been a long-reigning misunderstanding of the phrase 'scope of the management system', where people had confused it with 'scope of a certification audit'. There is a note to the definition of the term 'management system' in Annex SL which says 'The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations'. This may unwittingly exacerbate such confusion if it is not realized that the words 'may include' should be understood to imply that there may be other things within the scope, and in particular things that are external to the organization. As discussed in Chapter 2, the scope of the management system will include everything that is of interest to the management system. Thus, as evidenced by the note to the definition of the term 'outsource' in Annex SL, outsourced functions and processes are

within the scope of the management system. However, these are unlikely to be included within the scope of a certification audit, which is generally just the organization.

If, on reflection, there are entities that ought to be included within the scope of the management system but were previously excluded, transitioning to an Annex SL conformant management system standard will provide a convenient opportunity to redefine the scope.

XXX objectives

Similarly, a difference of opinion exists on whether the term 'objective' is a general aim or a specific goal that should be met within a specified time frame. Hopefully, Annex SL clarifies the fact that it can be both (i.e. both interpretations are correct) by the use of the phrase 'relevant functions and levels' in Subclause 6.2.

However, for an organization that thought of its XXX objectives as only being timeless policy objectives, the requirement of Subclause 6.2 may come as a shock. Nevertheless, it may only require a change to the way conformance is described as it is likely that an organization already sets objectives at all relevant functions and levels, and it is only just a question of recognizing that it does and describing how it does it.

For example, it is good practice when placing actions to define objectives, assign responsibilities and set target dates for completion. If an organization already does this, then it already conforms to this clause.

New requirements likely to be satisfied already

Nature of challenges

There are some new requirements in Annex SL, but it is likely that these will already be met by many organizations. In such cases, an organization merely needs to determine how it complies and then add a small amount of documented information, which ought to be readily available, to the transitioned management system. As mentioned in the section on 'choice of documentation media' in Chapter 3, organizations should not duplicate this information, but merely reference it.

Interested parties and their requirements

Subclause 4.2 requires an organization to determine the interested parties that are relevant to the XXX management system, and their requirement. It is highly likely that an organization already knows this

information. For example, interested parties may include customers and suppliers, and their requirements will be documented in contracts, purchase orders and specifications, etc. Thus, all that needs to be done is identify where this information is documented and reference it. It is also highly likely that the organization already makes use of this information thereby providing conformance with other subclauses such as 6.1.

Integration

The Annex SL integration requirement is in Subclause 5.1 ('ensuring the integration of the XXX management system requirements into the organization's business processes'). If the business functions of an organization are represented by a set of one or more work flow diagrams then if the activities that correspond to the management system requirements are spread throughout such work flow diagrams, then the integration requirement is probably met. Conversely, if the management system requirements are contained in a single work flow which contains nothing else, then the integration requirement is probably not met.

In the first case, it is then a question of how best to demonstrate conformance. If work flow diagrams exist, or can be visualized, e.g. through a software interface, then that would be an easy way to demonstrate conformance. If the integration requirement is not met, then the work flow concept may provide a route to achieving conformance.

New requirements that may present a challenge

Nature of challenges

Following on from above, there are some new requirements for which the required documented information probably does not exist and requires some thought and perhaps lateral thinking to create it. There are two areas that fall into this category: issues, and monitoring, measurement, analysis and evaluation.

Issues

It is likely that the issues referred to in Subclause 4.1 would be well-known to an organization, but not necessarily written down and certainly not in a way which would readily demonstrate conformance.

An important issue for most organizations would be its motivation for having a management system. An organization would, of course, know

what that was and it would have been a major driver in how the original management system has been designed. Note that this motivation may have changed over time: the original motivation being superseded by another as the benefits of having a management system are realized.

Another important issue would be those concerned with the XXX discipline itself, e.g. quality issues or environmental issues. If these are unknown or the organization is otherwise uncertain of them, it may be possible to reverse engineer them from a consideration of the XXX policy, objectives and the responses to particular discipline-specific requirements (e.g. planning of product realization for ISO 9001, business impact analysis for ISO 22301 and information security risk assessment and risk treatment for ISO/IEC 27001).

Other issues, which are likely to have already been addressed by an organization would relate to the operation of the management system, such as management commitment and staff motivation. Finally, organizations should consider looking through management meeting minutes and its records of preventive actions for further issues.

Monitoring, measurement, analysis and evaluation

The requirements of Subclause 9.1 are far more detailed and exacting than anything that may be deemed similar in any pre-Annex SL conformant management system standard. If there are discipline-specific requirements, such as customer feedback in ISO 9001, that are largely unchanged in the revised standard, then these are clear candidates for something that the organization can declare a topic for monitoring, measurement, analysis and evaluation as it is something that it already does. Staff competence is another example. However, Chapter 3 recommends that organizations do not monitor and measure just because the organization has the capability to do so: there must be a reason and that, as explained in Chapter 3, is the information need. Organizations are therefore strongly advised to follow the advice given in Chapter 3.

Areas where an organization may take the opportunity to improve

During the course of transitioning, an organization may find one or more opportunities for improvement. These are just as, if not more, likely to relate to discipline-specific requirements as they are to the identical core text requirements. Once identified, organizations need to decide whether to make the changes immediately, or highlight them as opportunities for improvement with the intention of making the changes at an appropriate time in the future.

The first course of action is more typical if the organization is using the transition as a reason for making other changes, while the second is used if the organization has adopted a minimalistic transition strategy.

Summary

Transition strategy

Transitioning using the minimalistic strategy can be accomplished quite quickly, and given the improvement likely to the discipline-specific requirements in a revised standard, organizations are encouraged to transition as soon as they can rather than put off transitioning to the latest possible time. However, once detailed planning for transition is underway, organizations may well encounter an overwhelming desire to make improvements, which is good.

Documented information

The change of nomenclature can be readily resolved by realizing that reference to documents in non-Annex SL standards are statements of intent whereas records concern evidence of past performance.

Preventive action

Existing procedures will need to be revised. However, a simple change, combined with the changes for corrective action, would be to refer to 'action plans' rather than 'preventive action plans'.

Document names

It does not matter what the standard calls a document or refers to an item of documented information. An organization can always call it by another name, provided the relationship is known.

XXX policy

There are additional requirements for the XXX policy, which are simple, and for all organizations ought not exceed one A4 page of text in total.

Control of documentation and internal audit

No changes ought to be required, although minor adjustments may be required to the explanation of conformance. However, organizations should check for new discipline-specific requirements and deviations.

Terms of reference for top management, management review, responsibilities, awareness and improvement

Minor changes and additions are likely to be required in these areas.

Scope of the management system

It is possible that existing management system documentation confuses *scope of the management system* with the *scope of a certification audit*. Resolution of such confusion is straightforward.

Objectives

At first view this may appear to be a significant change if an organization is used only to setting high level timeless policy objectives. However, it is likely that the requirement to establish objectives at relevant functions and levels is already met, and all an organization needs to do is document what it does.

Interested parties

It is highly likely that an organization already has documented information that identifies the interested parties and documents their requirements. All that is then needed is to reference it.

Integration

The integration requirement will be met if the activities that correspond to the management system requirements are spread throughout the organization's business function work flows.

Issues

Issues are likely to be discovered through a consideration of:

1. the organization's motivations for having a management system;

2. issues concerned with the XXX discipline itself, e.g. quality issues or environmental issues;
3. issues relating to the operation of the management system, such as management commitment and staff motivation;
4. management meeting minutes; and
5. records of preventive actions.

Monitoring, measurement, analysis and evaluation

This is likely to be by far the greatest challenge of a transition. The advice given in Chapter 3 should be followed, and in particular not to monitor and measure just because the organization has the capability to do so: there must be a valid information need as the first few requirements in Subclause 9.1 are there to support the final requirement, which is to assess XXX performance and XXX management system effectiveness.

Opportunities for improvement

During the course of transitioning, an organization may find one or more opportunities for improvement. Treat these in accordance with the chosen transition strategy.

Bibliography

Standards publications

BS 7799-2:2002, *Information security management systems — Part 2: Specification with guidance for use*

BS 25999-2:2007, *Business continuity management — Part 2: Specification*

ISO 9001:2000 and 2008, *Quality management systems — Requirements*

ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*

ISO 22000:2005, *Food safety management systems — Requirements for any organization in the food chain*

ISO 22301:2012, *Societal security — Business continuity management systems — Requirements*

ISO/IEC 27001:2005 and 2013, *Information technology — Information security management systems — Requirements*

ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management measurements*

ISO/IEC 27013:2012, *Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*

ISO/IEC Directives, Part 1 — *Consolidated ISO Supplement* (3rd Edition)

PAS 99:2012, *Specification of common management system requirements as a framework for integration*

Other publications

[a]Brewer, D.F.C., Nash, M.J. and List, W. (2005) Exploiting an integrated management system, available at: http://www.gammassl.co.uk/research/MSExploitation.pdf [accessed September 2013]

[b] Brewer, D.F.C. (2004) A tale of BS 7799-2 certification, available at: http://www.gammassl.co.uk/research/archives/ISMS/Certification%20v02.pdf [accessed September 2013]

Understanding the New ISO Management System Requirements

In April 2012, ISO updated its directives. In particular, there is a new annex - Annex SL - in which Appendix 3 defines the High Level Structure and Identical Core Text for all new and revised management system standards. The concept is that some requirements, e.g. management review, are common to all management system standards and therefore ought to be identically worded.

The book explains the new requirements and how they are related to those in management system standards published prior to the advent of the new ISO directives. In so doing it shows how familiar concepts have metamorphosed into new ones. It provides fresh insights into understanding management system standards and thereby gives guidance on how to develop a management system for the first time. It gives advice on transitioning existing management systems to the new requirements and on the construction and use of integrated management systems.

The book is aimed primarily at people who engage in creating and running management systems, including management system administrators, consultants, trainers and auditors.

No prior knowledge of management systems is assumed.

About the author

Dr David Brewer has a long history of involvement with quality systems beginning in 1980 when he acted as quality assurance section leader on a large software intensive project. He became involved with standards writing in the late 1980s and became a co-author of the original ISMS standard, BS 7799 Part 2, and is now an active member of the UK delegation to ISO JTC 1 SC27 WG1 which is responsible for the ISO 27000 family of standards; and is co-editor for the revision of ISO/IEC 27004 (Measurements). He has played a significant role in the revision of ISO/IEC 27001 and its conformance to the new ISO directives on High Level Structure and Identical Core Text.

He has conducted a wide variety of consultancy assignments spanning 32 years in over 23 countries. He is well known for his work in rolling out ISO/IEC 27001 to the whole of the Civil Service in Mauritius, which is an exemplar of his ISMS implementation methodology. Dr Brewer runs an integrated management system, which conforms to the quality, business continuity and information security management system standards. His seminal research papers include *'Measuring the Effectiveness of an Internal Control System'*, published in 2003 and *'Exploiting an Integrated Management System'*, published in 2005.

BSI order ref: BIP 0140

ISBN 978-0-580-82166-0

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL
www.bsigroup.com

© BSI copyright

Understanding the New ISO Management System Requirements

David Brewer