Understanding the New ISO Management System Requirements

Dr David Brewer
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>vii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>ix</td>
</tr>
<tr>
<td><strong>Chapter 1 – The new ISO management system requirements</strong></td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Motivation</td>
<td>1</td>
</tr>
<tr>
<td>High level structure</td>
<td>3</td>
</tr>
<tr>
<td>Identical core text</td>
<td>4</td>
</tr>
<tr>
<td>Deviations</td>
<td>4</td>
</tr>
<tr>
<td>Discipline-specific text</td>
<td>5</td>
</tr>
<tr>
<td><strong>Chapter 2 – Management system concepts</strong></td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Definitions</td>
<td>6</td>
</tr>
<tr>
<td>What is a management system?</td>
<td>9</td>
</tr>
<tr>
<td>How management systems work</td>
<td>10</td>
</tr>
<tr>
<td>Understanding management system standards</td>
<td>14</td>
</tr>
<tr>
<td>Evolution of management system concepts</td>
<td>16</td>
</tr>
<tr>
<td>Integrated management systems</td>
<td>18</td>
</tr>
<tr>
<td><strong>Chapter 3 – Understanding the new requirements</strong></td>
<td>20</td>
</tr>
<tr>
<td>Introduction</td>
<td>20</td>
</tr>
<tr>
<td>Whatever happened to PDCA?</td>
<td>20</td>
</tr>
<tr>
<td>Discipline-specific requirements</td>
<td>22</td>
</tr>
<tr>
<td>Scope of the management system</td>
<td>22</td>
</tr>
<tr>
<td>Policy and objectives</td>
<td>28</td>
</tr>
<tr>
<td>Risks and opportunities</td>
<td>31</td>
</tr>
<tr>
<td>Operation</td>
<td>32</td>
</tr>
<tr>
<td>Monitoring, measurement, analysis and evaluation</td>
<td>34</td>
</tr>
<tr>
<td>Audits and reviews</td>
<td>40</td>
</tr>
<tr>
<td>Management and support</td>
<td>46</td>
</tr>
<tr>
<td>Implementation guidance</td>
<td>57</td>
</tr>
<tr>
<td><strong>Chapter 4 – Transitioning to the new management system</strong></td>
<td>63</td>
</tr>
<tr>
<td>Introduction</td>
<td>63</td>
</tr>
<tr>
<td>Transition strategies</td>
<td>63</td>
</tr>
<tr>
<td>Integrated management system considerations</td>
<td>64</td>
</tr>
<tr>
<td>Areas requiring little or no change</td>
<td>66</td>
</tr>
</tbody>
</table>

---

*This is a sample chapter from Understanding the new Management System Requirements.*  
To read more and buy, visit [http://shop.bsigroup.com/BIP0140](http://shop.bsigroup.com/BIP0140)  
© The British Standards Institution 2013
Areas that potentially require a rethink
New requirements likely to be satisfied already
New requirements that may present a challenge
Areas where an organization may take the opportunity to improve
Summary

Bibliography
Standards publications
Other publications
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. 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.

Dr 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.


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
Chapter 1 – The new ISO management system requirements

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.