



ANNEXSL

THE GREAT OPPORTUNITY

Briefing note



Contents

03 Foreword

04 Introduction and consequences

05 Overview

06 Applicability

07 Identical core text

11 Migration

12 Bibliography

Published in April 2015 by the International Register of Certificated Auditors (IRCA), part of the Chartered Quality Institute (CQI): 2nd Floor North, Chancery Exchange, 10 Furnival Street, London, EC4A 1AB.

© CQI 2015. All rights reserved.

Incorporated by Royal Charter and registered as a charity, number 259678



“The most important management system event since the launch of ISO 9001”

Richard Green, Head of Technical Services

In December 1987, ISO 9001 quality systems model for quality assurance in design, development, production, installation and servicing was published.

It was the start of a global phenomenon that, over the course of the past three decades, has seen an exponential rise in the number of management system standards and accredited certifications – approaching 1.6 million*.

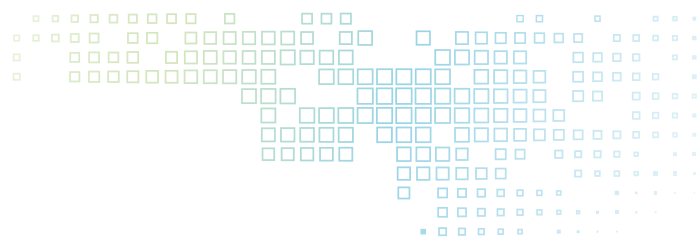
There is no doubt that ISO 9001 has played a significant role in shaping the management system standards world, so to suggest that something new has come along to rival ISO 9001's introduction requires further explanation. But what is this game changer that is going to have a significant impact on organisations, trainers, consultants, certification bodies, accreditation bodies, auditors and management system writers alike? Well, it's the rather innocuously titled Annex SL.

Annex SL and its associated appendices collectively define a generic management system framework. In the future, all new ISO management system standards will adhere to the framework and all current management system standards will migrate to it at their next revision.

As a result of the introduction of Annex SL, all ISO management system standards should become more consistent in time, and hence more compatible. They will share the same look and feel, having been built on a common foundation. Annex SL represents the beginning of the end of the conflicts, duplication, confusion and misunderstanding arising from subtly different requirements across the various management system standards.

Auditors now face the challenge of focusing their own, and their clients', thinking on viewing organisations' management systems holistically.

**The ISO Survey 2013*



Introduction

The ultimate prize for any organisation seeking to implement multiple management system standards is a truly integrated system, but historically this has proved elusive. Although requirements across management system standards are often broadly similar, subtle (and in some cases not so subtle) differences have led to organisations having to deliberately introduce duplication, and hence operational inefficiencies, in order to maintain conformity. As the number of management system standards continued to grow, the potential for conflicts grew with it. ISO recognised that something had to be done and that something was Guide 83, which later transformed into Annex SL.

Annex SL describes the framework for a 'generic' management system. In order to become a fully functional, discipline-specific management system, discipline-specific requirements must be added (by the standard writers) to the generic requirements contained in Annex SL Appendix 2.

Consequences

In future all new management system standards will have the same overall look and feel. Current management system standards will migrate during their next revision and this should be completed within the next few years.

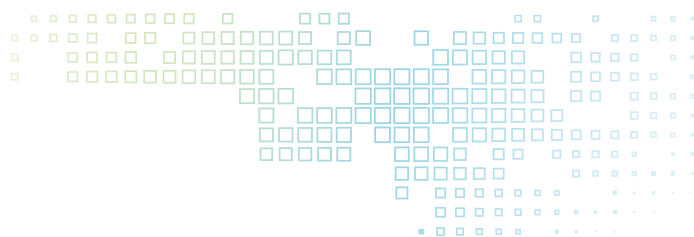
For management system standards writers, Annex SL will provide the template for their work and they can concentrate their efforts on the discipline-specific requirements that will be focused on in Clause 8 – Operation.

For management system implementers this will provide an overall management system framework within which they can pick and choose what discipline-specific standards they wish to include. Gone will be the conflicts, duplication, confusion and misunderstanding arising from different management system standards. In future, all ISO management system standards should be consistent and compatible.

For management system auditors, it will mean that for all audits there will be a core set of generic requirements that need to be addressed – no matter what discipline is being examined. For IRCA training it could drive the development of training addressing the common core set of requirements, with additional training for discipline-specific requirements being undertaken as a separate or supplementary module.

“In future, all ISO management system standards should be consistent and compatible... they will have the same overall look and feel”

Overview



Annex SL addresses the requirements for proposals for management system standards. It consists of nine clauses and three appendices, and the audience for this annex is primarily ISO technical committees who develop management system standards. However, all users of management system standards will feel the impact of Appendix 2 of Annex SL in the future. Appendix 2 is in three parts:

- High-level structure
- Identical core text
- Common terms and core definitions.

All management system standards will need to have these elements. There will be less confusion and inconsistency as all common terms will have the same definition, and there will be common requirements across all management system standards. For example, the requirement to establish, implement, maintain and improve continually the management system.

But what changes can and can't be made? The high-level structure (ie major clause numbers and titles) cannot be changed. However, sub-clauses and discipline-specific text can be added. For example:

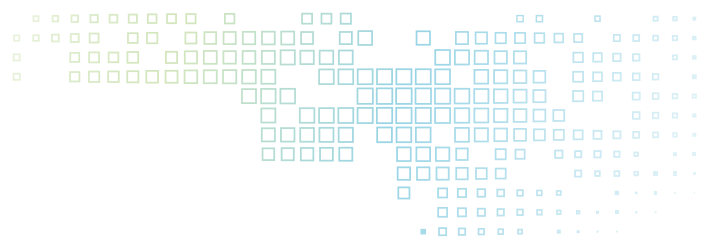
- New bullets
- Discipline-specific notes or examples
- Discipline-specific new paragraphs to sub-clauses
- Adding text that enhances (but does not modify) the existing requirements.

The common terms and core definitions cannot be changed. However, terms and definitions may be added as needed, and notes may be added or modified to serve the purpose of each standard.

To facilitate the adoption of the core text, the device 'XXX' is used. Throughout Annex SL, for 'XXX' the appropriate reference needs to be inserted – ie in ISO 22000 the 'XXX' needs to be replaced with 'food safety' and in ISO 14001 the 'XXX' needs to be replaced by 'environmental'. In addition, the term 'discipline' is used to describe the nature of the management system – ie quality, environmental, service management, food safety, business continuity, information security or energy.

Note: In this briefing note, the management system is the XXX management system referred to in Annex SL.

Applicability



This annex applies to all management system standards – full ISO standards, technical specifications (TS) and publicly available specifications (PAS), but not to international workshop agreements (IWA). Examples of the standards it applies to are:

- ISO 14001:2004 environmental management systems – requirements with guidance for use
- ISO/TS 16949:2009 quality management systems – requirements for the application of ISO 9001:2008 for automotive production and relevant service part organisations.

Examples of standards that it does not apply to:

- ISO 19011:2011 – guidelines for auditing management systems
- IWA 2:2007 quality management systems – guidelines for the application of ISO 9001:2000 in education.

High-level structure

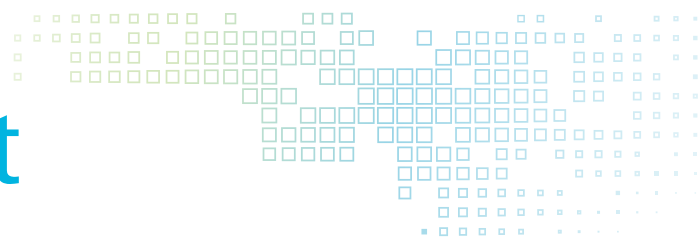
The major clause numbers and titles of all management system standards will be identical. They are:

Introduction

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

The introduction, scope and normative references will have content that are specific to each discipline, and each standard can have its own bibliography.

All management system standards will have these same 10 high-level clauses in the order listed above, irrespective of the discipline the standard relates to – ie in every management system standards Clause 5 there will always be 'leadership'. Where previous requirements have been carried forward into new Annex SL-based standards, these are often found under new clause headings. As such it will take a little while for those using management system standards to become familiar with navigating their way around the latest releases. However, once this is mastered, the individual will be able to find their way quickly around all management system standards.



Identical core text

Think of core text as a Microsoft Word template containing text that is fixed and can't be edited. Standard-specific text can be added (by standard writers) to the core text, but the core text itself can't be amended or deleted. It must appear 'as is' in all Annex SL-based management system standards. In the current version of Annex SL Appendix 2, 45 'shall' statements (generating 84 requirements) appear as core text. This means, as a minimum, Annex SL-based standards must contain 84 requirements. In practice the number will be higher as standard writers will want to add in their own discipline-specific requirements too.

Detailed content:

1. Scope

The scope should define what the 'intended outcome(s)' are of the discipline. The term 'expected outcome' will not be used. Auditors should expect to evidence alignment between what the organisation has determined in Clause 4 with what is stated here.

4. Context of the organisation

- 4.1 Understanding the organisation and its context
- 4.2 Understanding the needs and expectations of relevant parties
- 4.3 Determining the scope of the XXX management system
- 4.4 XXX management system.

At first glance, Clause 4 is radical and daunting, but on further consideration it makes sense in practice. The organisation will already have completed this thinking before even considering implementing any ISO management system. This is the flagstone of the management system – why the organisation is here. The organisation needs to determine its relevant issues, both inside and outside, that have an impact on what it is trying to achieve – ie its intended outcomes. Also, who are the relevant interested parties (the preferred term to stakeholders) and what are their relevant requirements (the requirements that impact the organisation's management system)?

The organisation needs to determine and document its own scope – where are the boundaries of the management system? What's in and what's out? The scope must be appropriate to the organisation and its objectives, and the organisation also needs to build, operate and improve its management system. The issues and requirements identified here will be carried forward as considerations into Clause 6 – Planning.

Auditors should now have a clear and concise list of objective evidence to identify and confirm. It will include the organisation's goals and intended outcomes, internal and external issues, relevant stakeholders and their relevant requirements, and the management system scope. Collectively, this will provide a key insight into the organisation and its interaction with the wider world.

5. Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organisational roles, responsibilities and authorities.

At first glance, Clause 5 appears to be just a reiteration of what's gone before – ie the requirement for policy and definition of organisational roles, responsibilities and authorities. However, there is now a clear emphasis on leadership, not management, and these are not one and the same but very different things. On further examination, it becomes clear that this clause has potentially the most far-reaching implications of any of the Annex SL-induced changes. Top management, those at the highest level in the organisation, now have to demonstrate much greater involvement in the operation of the organisation's management system(s).

They have to make sure that the requirements of the management system are integrated into the organisation's business processes and that the management system isn't just a bolt-on. They also have to demonstrate their commitment by making sure that the management system achieves its intended outcome(s) and has adequate resources, as well as informing everyone of its importance and why they should participate in its effective implementation. The involvement from top management in the management system is now explicit and hands-on – actions that they cannot delegate. As such, top management can expect to be routinely audited in order to ensure that they are fulfilling their obligations.

The XXX policy has also been strengthened. It has to include commitments to satisfy applicable requirements and improve continually the management system, and as well as being communicated internally, it has to be made available to all relevant and interested parties.

Auditors should now find it easier to audit commitment. The requirements are much more specific and tangible, and the evidence required should be more obvious.

6. Planning

6.1 Actions to address risks and opportunities

6.2 XXX objectives and planning to achieve them.

After much deliberation, the decision to make risk explicit has been made – here it is in Clause 6. Having highlighted the issues and requirements in Clause 4, now is the time to address the risks and opportunities organisations face by means of 'planning'. How will the organisation prevent or reduce undesired effects? How will it ensure it can achieve its intended outcomes and improvement continually? It will do it here, in planning.

Planning will address what, who, how and when – it's not difficult. This proactive approach is easier to understand than preventative action and should reduce the need for correction and corrective action at a later date.

The requirements around the XXX objectives have also been made more detailed. They are to be consistent with the XXX policy, measurable (if practicable), monitored,

communicated and updated as appropriate. They have to be established at relevant functions and levels. Clause 6 puts a greater emphasis on the organisation's XXX planning, which is integral to the business.

Auditors should be familiar with risk – “the consequences of an event and the associated likelihood of occurrence” – and how to avoid, eliminate, minimise or mitigate it. They also need to focus on the positive aspect, opportunities for the business, and how to optimise them. The risks and opportunities identified will lead to policies and objectives. Auditors should be able to identify and follow a clear path from issues and requirements through to risks and opportunities, policies and objectives.

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.

Having addressed context, leadership and planning, it's now time to provide the support required to meet organisational goals. The organisation needs to supply competent resource to deliver its goods and services, so again, nothing new here. Awareness has been strengthened and now everyone needs to know the implications of not conforming to the management system requirements.

The organisation needs to consider the need for both internal and external communications relevant to the management system – what, when and with whom it will communicate – as well as how it will communicate.

The final support requirement is going to generate a lot of heat but not much light – documented information. Gone are the terms documents, documentation and records. However, the requirements for the management of documented information are not new, exceptional or excessive. One ghost that is finally laid to rest is the idea that everyone needs work instructions, no matter how experienced or senior they are in the organisation (see the note in Clause 7.5.1).

Auditing awareness and communication should be easier. The requirements are crisper and auditors should find the consistent definition of, and requirements for competence, a benefit.

Auditors will need to understand and use the term 'documented information'. Although there will be a lot of confusion and misunderstanding as everyone transitions from the old terms, in the long run they should benefit from the greater clarity and consistency.

8. Operation

8.1 Operational planning and control.

Whatever the organisation is in business to achieve, Clause 8 is it. At its core, the organisation needs to “...plan, implement and control the processes needed”.

This addresses both in-house and any outsourced processes. The overall process management includes having process criteria, controlling the processes within the criteria, planned change and addressing unintended change as necessary.

This is the shortest Annex SL Appendix 2 clause because this is where the bulk of each discipline – the XXX requirements – will be. It’s also where the need for a discipline-specific management system model will come from.

The auditor will have to have a good understanding of process management before getting involved in assessing the discipline-specific requirements. This is where an understanding of the business context of Clause 4 will bear fruit – the sharp end of the business operations.

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review.

Having ‘done the business’ in Clause 8, it’s time to check performance and the usual suspects appear here. The organisation determines what, how and when things are to be monitored, measured, analysed and evaluated. Add internal audit and management review to the mix and everything expected is addressed.

Internal audits carried out by the organisation, or by an external party acting on the organisation’s behalf, provide information on whether the management system conforms to the requirements of the organisation and the standard, and whether it is effectively implemented and maintained. Management review addresses the question: is the management system suitable, adequate and effective?

Once again, the auditor should benefit from a consistent set of requirements for checking results against plan. There is a long list of objective evidence that can be identified and confirmed – metrics, schedules, evaluations, nonconformities, corrective actions, monitoring and measurement results, and audit and management review results.

10. Improvement

10.1 Nonconformity and corrective action

10.2 Continual improvement.

Occasionally undesired things occur and now it's time to address nonconformity and corrective action, and to make things better there is also continual improvement. The requirements here are familiar and well understood, but what about preventative action? It does not appear. As some have argued for many years, one of the objectives of a management system is preventative action.

The requirements in Clause 4.1 to "...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", and in Clause 6.1 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," not only addresses preventative action but goes beyond. And in the end, auditors will look back at the management system established in Clause 4.4, reviewed in Clause 9.3, and now improved continually.

Finally, although there remains a requirement for processes (see Clause 4.4), there is no mention anywhere of procedures – documented or otherwise. If a discipline considers that they are required then they will appear in the XXX standard, probably in Clause 8 – Operations. However, if they are not a requirement but the organisation considers it needs them, then that will be its decision.

Migration

The migration of most of the current management system standards should not prove arduous.

ISO 22301:2013 societal security – business continuity management systems – requirements developed using a draft version of Annex SL. See IRCA briefing note on business continuity

ISO 27001 information technology – security techniques – information security SL, **ISO 9001:2008** quality management systems – requirement, and **ISO 14001:2004** – environmental management systems – are currently being revised using the published version of Annex SL.

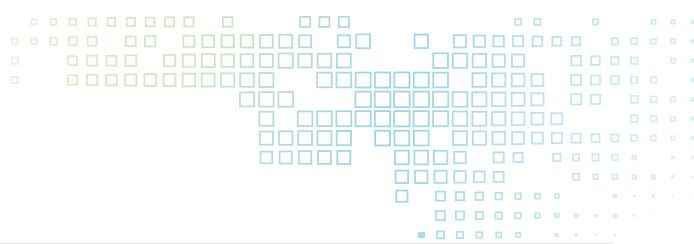
ISO 22000:2005 food safety management systems – requirements for any organisation in the food chain will be addressing the requirements of Annex SL Appendix 2 during their interim revision cycle.

Service management and energy management system standards, both published recently, will need to consider whether to issue a revision soon or wait for the next full revision cycle. The International Register of Certificated Auditors (IRCA) has prepared

this briefing note to communicate to IRCA Certificated Auditors, IRCA Approved training organisations and other interested parties, our understanding of Annex SL of the ISO/IEC Directives, Part 1 Consolidated ISO Supplement – procedures specific to ISO.

The content of this briefing note is provided in good faith and is the opinion of IRCA. It should not be reproduced nor used for commercial purposes. IRCA Certificated Auditors and IRCA Approved training organisations are advised to familiarise themselves with Annex SL.

Bibliography



- 01** ISO 9000:2005 quality management systems – fundamentals and vocabulary
- 02** ISO 9001:2008 quality management systems requirements
- 03** ISO 14001:2004 environmental management systems – requirements with guidance for use
- 04** ISO/IEC 20000-1:2011 information technology – service management – part 1: service management system requirements
- 05** ISO 22000:2005 food safety management systems – requirements for any organisation in the food chain
- 06** ISO 22300:2012 societal security – terminology
- 07** ISO 22301:2012 societal security – business continuity management systems – requirements
- 08** ISO/IEC 27000:2014 information technology – security techniques – information security management systems – overview and vocabulary
- 09** ISO/IEC 27001:2013 information technology – security techniques – information security management systems – requirements
- 10** ISO 50001:2011 energy management systems – requirements with guidance for use.

Published by:
The International Register
of Certificated Auditors (IRCA)
Part of: The Chartered Quality Institute

The Chartered Quality Institute (CQI)
2nd Floor North, Chancery Exchange
10 Furnival Street
London EC4A 1AB
United Kingdom

T: +44 (0) 20 7245 6722
F: +44 (0) 20 7245 6788
thecqi.org irca.org

Incorporated by Royal Charter and
registered as a charity number 259678
© 2015 the CQI. All Rights Reserved

ANNEXSL
THE GREAT OPPORTUNITY