

IRCA briefing note

Annex SL



The most important event since ISO 9001?



A quarter of a century ago, in December 1987, 'ISO 9001 Quality systems – Model for quality assurance in design/development, production, installation and servicing' was published. This was the start of a global phenomenon which saw the range of ISO management system standards (MSS) expand through environment (1996) through to asset management (2014) and accredited certifications approach 1.5 million.*

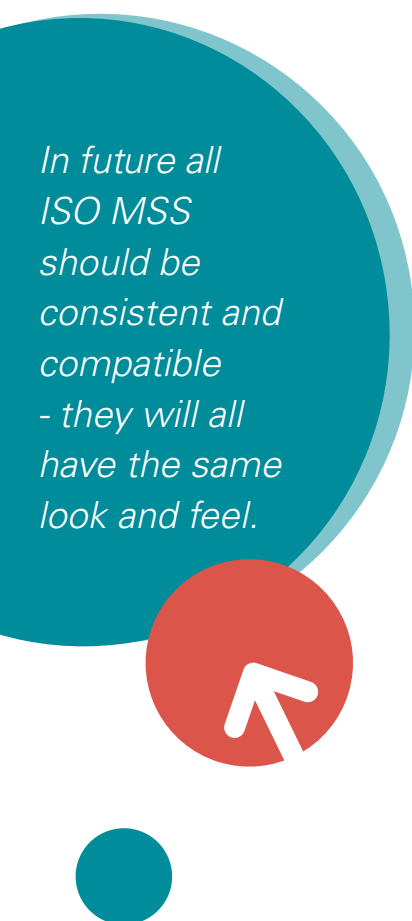
So what is this event that will have such a significant impact on organisations, trainers, consultants, certification bodies, accreditation bodies, auditors and MSS writers? It is the publication of Annex SL (previously ISO Guide 83) which defines the framework for a generic management system. All new ISO MSS will adhere to this framework and all current MSS will migrate to the framework at their next revision.

In future all ISO MSS should be consistent and compatible - they will all have the same look and feel. This could be the beginning of the end of the conflicts, duplication, confusion and misunderstanding arising from subtly different requirements across the various MSS.

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

*The ISO Survey 2010





*In future all
ISO MSS
should be
consistent and
compatible
- they will all
have the same
look and feel.*

Introduction

Many organisations seek to implement and certify multiple management system standards. This has led to the need to easily combine or integrate them in an effective and efficient manner. To date subtle and not so subtle differences in requirements and terminology across MSS have made such integration difficult. ISO/TMB has produced Annex SL with the objective of delivering consistent and compatible management system standards in an attempt to make this process easier.

Annex SL describes the framework for a generic management system. However, it will require the addition of discipline-specific requirements to make a fully functional quality, environmental, service management, food safety, business continuity, information security and energy management system standard. Annex SL is freely available; it is contained within the ISO Supplement, Procedures specific to ISO.

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. This should be completed within the next few years.

For management system standards writers Annex SL will provide the template for their work. They can concentrate their efforts on the discipline-specific requirements which will be focused on 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 and 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 which 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.

Overview

Annex SL addresses the requirements for proposals for management system standards. It consists of 9 clauses and 3 appendices. The audience for this annex is primarily ISO technical committees who develop management system standards; however the impact of Appendix 2 of Annex SL will be felt by all users of management system standards in the future. Appendix 2 is in three parts:

- high level structure,
- identical core text,
- common terms and core definitions.

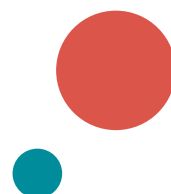
In future all management system standards will need to have these elements. In addition, there will be less confusion and inconsistency because common terms will all have the same definition and there will be common requirements across all the management system standards, for example the requirement to establish, implement, maintain and continually improve the management system. So what changes can and cannot be made? The high level structure (i.e. major clause numbers and titles) cannot be changed, however sub-clauses can be added. Discipline-specific text can also be added; for example:

- new bullets
- discipline-specific explanatory text (e.g. 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; for example in ISO 22000 'XXX' needs to be replaced by "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 i.e. 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 standards that it applies to are:

- ISO 14001:2004 Environmental management systems - Requirements with guidance for use
- ISO/TS 16949:2009 Quality management systems - Particular 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 are:

- 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 organisation
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.

Overall there is a reorganising of management system requirements into this structure that may be unfamiliar to those using and assessing current MSS. However, some management system standards (such as ISO 22301:2012 Societal security - Business continuity management systems - Requirements) have already successfully migrated to this new structure.

Identical core text

There are 45 “shall” statements (generating 84 requirements) in Annex SL Appendix 2, therefore there must be at least 45 “shall” statements with 84 requirements in all future management system standards. Obviously each discipline will have their own requirements, so the total for any new standard will have more – this is the minimum.

The detailed content is:

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 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 interested 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 have 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, its intended outcomes.

Also, who are the relevant interested parties (the preferred term to stakeholders) and what are their requirements?

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? This must be needs to be appropriate to the organisation and its objectives. Finally, the organisation needs to build, operate and improve its management system; nothing new or difficult there. The issues and requirements identified here will be addressed in clause 6 - Planning.

Auditors should now have a clear and concise list of objective evidence to identify and confirm. It will include the organisations goals and intended outcomes, internal and external issues, the relevant stakeholders and their requirements and the management system scope. Collectively this will provide a key insight into the organisation. This should not be just a tick-list, but the entirety will provide a key insight into the organisation - it should provide illumination and clarity.

5. Leadership

- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 organisational roles, responsibilities and authorities



Identical core text (continued)

Again, at first glance, clause 5 appears to be just a reiteration of what's gone before –policy, organisational roles, responsibilities and authorities etc. However, there is an emphasis on leadership, not just management. On further examination there is more here; top management now have to have a greater involvement in the management system.

They have to make sure that the requirements of the management system are integrated into the organisation's business processes – the management system is not just a bolt-on. The 'business' is whatever activities are at the heart of the organisation's reason for existing.

In addition, they have to demonstrate their commitment by making sure that the management system achieves its intended outcome(s) and has adequate resources. Additionally they have to inform everyone that management system is important and that everyone should participate in its effective implementation. The involvement of top management in the management system is now explicit and hands-on.

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

Auditors should now find it easier to audit management 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 it is time to address the risks and opportunities the organisation faces through planning.

How will the organisation prevent, or reduce, undesired effects? How will the organisation ensure that it can achieve its intended outcomes and continual improvement? It will do it here in planning. Planning will address what, who, how and when. Not difficult. This proactive approach is easier to understand than preventive 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 optimize 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 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 the context, commitment and planning it is now time to provide the support required to meet the organisation's goals. The organisation needs to supply competent resource to deliver its goods and services. Again, nothing new here, awareness has been strengthened so 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.

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 skeleton which is finally laid to rest is the idea that everyone needs work instructions no matter how experienced or senior they are in the organisation (check out the Note in clause 7.5.1).

Auditing awareness and communication should be easier; the requirements are crisper – the 3 W's. Again, 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 auditors 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. This overall process management includes having process criteria, controlling the processes within the criteria, controlling planned change and addressing unintended change as necessary.

This is the shortest clause because this is where the bulk of each discipline - the 'XXX' - requirements will be. It is also where the need for a discipline-specific management system model will come from. So where will all the requirements go that don't fall easily into the High level Structure and Identical core text? For example in ISO 9001:2008 7.3.4 Design and development review and in ISO 14001: 2004 4.4.7 Emergency preparedness and response. Whatever is at the heart of the 'XXX' management system – 'the business' – then this is what goes into clause 8.





Identical core text (continued)

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 is time to check performance. 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 provide information on whether the management system conforms to the requirements of the organisation and the standard and 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 and 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; now it's time to address nonconformity and corrective action. And to make things better there's continual improvement. The requirements here are familiar and well understood. But what about preventive action? It does not appear. As some have argued for many years, one of the objectives of a management system is preventive 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 address preventive action but go 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 continually improved.

Finally, although there remains a requirement for processes (check out 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 themselves consider they need them then that will be their 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 was developed using a draft version of Annex SL. See IRCA briefing note on business continuity.

ISO 27001 Information technology - Security techniques - Information security management systems – Requirements was developed using the published version of Annex SL.

ISO 9001:2008 Quality management systems – Requirements has started its revision cycle and is being developed using the published version of Annex SL. The environmental management and food safety management system standards will be addressing the requirements of Annex SL Appendix 2 during their interim revision cycle.

Service management and energy management system standards, which were 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

- [1] ISO 9000:2005 Quality management systems - Fundamentals and vocabulary
- [2] ISO 9001:2008 Quality management systems Requirements
- [3] ISO 14001:2004 Environmental management systems - Requirements with guidance for use
- [4] ISO/IEC 20000-1:2011 Information technology - Service management - Part 1: Service management system requirements
- [5] ISO 22000:2005 Food safety management systems - Requirements for any organisation in the food chain
- [6] ISO 22300:2012 Societal security - Terminology
- [7] ISO 22301:2012 Societal security - Business continuity management systems - Requirements
- [8] ISO/IEC 27000:2014 Information technology - Security techniques - Information security management systems - Overview and vocabulary
- [9] 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



**International Register of
Certificated Auditors (IRCA)**

2nd Floor North, Chancery Exchange
10 Furnival Street
London EC4A 1AB
United Kingdom

E: registration@irca.org

T: +44 (0) 20 7245 6833

F: +44 (0) 20 7245 6755

www.irca.org



Follow the IRCA on Twitter
www.twitter.com/irca_inform



Follow our company updates on LinkedIn
www.linkedin.com