Appendix 2

(normative)

High level structure, identical core text, common terms and core definitions

NOTE In the Identical text proposals, XXX = an MSS discipline specific qualifier (e.g. energy, road traffic safety, IT security, food safety, societal security, environment, quality) that needs to be inserted. Blue italicized text is given as advisory notes to standards drafters.

Introduction

DRAFTING INSTRUCTION Specific to the discipline.

1. Scope

DRAFTING INSTRUCTION Specific to the discipline.

2. Normative references

DRAFTING INSTRUCTION Clause Title shall be used. Specific to the discipline.

3. Terms and definitions

DRAFTING INSTRUCTION 1 Clause Title shall be used. Terms and definitions may either be within the standard or in a separate document. To reference Common terms and Core definitions + discipline specific ones. The arrangement of terms and definitions shall be according to the concept systems of each standard.

For the purposes of this document, the following terms and definitions apply.

DRAFTING INSTRUCTION 2 The following terms and definitions constitute an integral part of the "common text" for management systems standards. Additional terms and definitions may be added as needed. Notes may be added or modified to serve the purpose of each standard.

DRAFTING INSTRUCTION 3 Italics type in a definition indicates a cross-reference to another term defined in this clause, and the number reference for the term is given in parentheses.

DRAFTING INSTRUCTION 4 Where the text "XXX" appears throughout this clause, the appropriate reference should be inserted depending on the context in which these terms and definitions are being applied. For example: "an XXX objective" could be substituted as "an information security objective".

3.01
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.08)

Note 1 to entry: 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.

3.02
interested party (preferred term)
stakeholder (admitted term)
person or *organization* (3.01) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.03
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "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.

Note 2 to entry: A specified requirement is one that is stated, for example in documented information.

3.04
management system
set of interrelated or interacting elements of an *organization* (3.01) to establish *policies* (3.07) and *objectives* (3.08) and *processes* (3.12) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.

Note 3 to entry: 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.

3.05
top management
person or group of people who directs and controls an *organization* (3.01) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.04) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.06
effectiveness
extent to which planned activities are realized and planned results achieved

3.07
policy
intentions and direction of an *organization* (3.01), as formally expressed by its *top management* (3.05)

3.08
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.12)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an XXX objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of XXX management systems, XXX objectives are set by the organization, consistent with the XXX policy, to achieve specific results.

3.09
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
documented information
information required to be controlled and maintained by an *organization* (3.01) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.04), including related *processes* (3.12);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.12
process
set of interrelated or interacting activities which transforms inputs into outputs

3.13
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.12), products (including services), systems or *organizations* (3.01).

3.14
outsource (verb)
make an arrangement where an external *organization* (3.01) performs part of an organization's function or *process* (3.12)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.04), although the outsourced function or process is within the scope.

3.15
monitoring
determining the status of a system, a *process* (3.12) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

3.16
measurement
process (3.12) to determine a value

3.17
audit
systematic, independent and documented *process* (3.12) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the organization itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.18
conformity
fulfilment of a *requirement* (3.03)

3.19
nonconformity
non-fulfilment of a *requirement* (3.03)

3.20
corrective action
action to eliminate the cause of a *nonconformity* (3.19) and to prevent recurrence

3.21
continual improvement
recurring activity to enhance *performance* (3.13)

4. Context of the organization

4.1 Understanding the organization and its context

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.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

— the interested parties that are relevant to the XXX management system;

— the relevant requirements of these interested parties.

4.3 Determining the scope of the XXX management system

The organization shall determine the boundaries and applicability of the XXX management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2.

The scope shall be available as documented information.

4.4 XXX management system

The organization shall establish, implement, maintain and continually improve an XXX management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard/this part of ISO XXXX/this Technical Specification.

5. Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the XXX management system by:

— ensuring that 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 of 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.

NOTE Reference to "business" in this International Standard/this part of ISO XXXX/this Technical Specification can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

Top management shall establish a XXX policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting XXX objectives;

c) includes a commitment to satisfy applicable requirements;

d) includes a commitment to continual improvement of the XXX management system.

The XXX policy shall:

— be available as documented information;

— be communicated within the organization;

— be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the XXX management system conforms to the requirements of this International Standard/this part of ISO XXXX/this Technical Specification;

b) reporting on the performance of the XXX management system to top management.

6. Planning

6.1 Actions to address risks and opportunities

When planning for the XXX management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

— give assurance that the XXX management system can achieve its intended outcome(s);

— prevent, or reduce, undesired effects;

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

   — integrate and implement the actions into its XXX management system processes;

   — evaluate the effectiveness of these actions.

6.2 XXX objectives and planning to achieve them

The organization shall establish XXX objectives at relevant functions and levels.

The XXX objectives shall:

a) be consistent with the XXX policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated;

f) be updated as appropriate.

The organization shall retain documented information on the XXX objectives.

When planning how to achieve its XXX 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.

7. Support

7.1 Resources

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

7.2 Competence

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its XXX performance;

— 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;

— retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

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.

7.4 Communication

The organization shall determine the internal and external communications relevant to the XXX management system, including:

— on what it will communicate;

— when to communicate;

— with whom to communicate;

— how to communicate.

7.5 Documented information

7.5.1 General

The organization's XXX management system shall include:

a) documented information required by this International Standard/this part of ISO XXXX/this Technical Specification;

b) documented information determined by the organization as being necessary for the effectiveness of the XXX management system.

NOTE The extent of documented information for a XXX management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons.

7.5.2 Creating and updating

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.

7.5.3 Control of documented information

Documented information required by the XXX management system and by this International Standard /this part of ISO XXXX/this Technical Specification shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the XXX management system shall be identified, as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

8. Operation

8.1 Operational planning and control

DRAFTING INSTRUCTION *This subclause heading will be deleted if no additional subclauses are added to Clause 8.*

The organization shall 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;

— keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

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

The organization shall ensure that outsourced processes are controlled.

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall 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.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the XXX performance and the effectiveness of the XXX management system.

9.2 Internal audit

9.2.1 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/this part of ISO XXXX/this Technical Specification;

b) is effectively implemented and maintained.

9.2.2 The organization shall:

a) plan, establish, implement and maintain an audit programme(s) including the frequency, methods, responsibilities, planning requirements and reporting, which 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;

e) retain documented information as evidence of the implementation of the audit programme and the audit results.

9.3 Management review

Top management shall review the organization's XXX management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

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 system;

c) information on the XXX performance, including trends in:

   — nonconformities and corrective actions;

   — monitoring and measurement results;

   — audit results;

d) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes to the XXX management system.

The organization shall retain documented information as evidence of the results of management reviews.

10. Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity and, as applicable:

   — take action to control and correct it;

   — deal with the consequences;

b) evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by:

   — reviewing the nonconformity;

   — determining the causes of the nonconformity;

   — determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the XXX management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the XXX management system.

Appendix 3

(informative)

Guidance on high level structure, identical core text, common terms and core definitions

Guidance on the high level structure, identical core text, common terms and core definitions is provided at the following URL:

Annex SL Guidance documents (http://isotc.iso.org/livelink/livelink?func=ll&objId=16347818&objAction=browse&viewType=1).