Annex SL – High Level Structure (HLS) Background and Overview

1 Introduction

ISO Management System (MS) standards now share a common structure, known as the High Level Structure (HLS). This is specified in Annex SL, which is one part of an ISO specification document. Established MS standards, such as ISO 9001, have all been revised to conform to the HLS and new MS standards all conform to the HLS. The HLS provides consistency and avoids duplication, to simplify the implementation and operation of an Integrated Management System (IMS) that manages two or more aspects of operations. Each MS standard consists of the following two components.

*(1) A common core body of headings and text, which ensures that **(A)** The standard contains an enhanced form of a STEEPLE (or PESTLE) Analysis and a SWOT Analysis, to **FORMULATE STRATEGIES** and **(B)** Its structure corresponds to the **PDCA (Plan-Do-Check-Act)** cycle.*

*(2) Additional text, which is specific to management of the particular aspect of operations, such as **Information Security**, **Business Continuity** or **Anti-Bribery** that the standard governs.*

2 Need for a Common Structure for MS Standards

A common structure for MS standards, to facilitate integration, is not a new concept. The following four MS standards shared a common structure. (Refer to Appendix 2.)

ISO 14001:2004 - Environmental Management Systems
OHSAS 18001:2007 - Occupational Health and Safety Management Systems
ISO 28000:2007 - Security Management Systems for the Supply Chain
ISO 50001:2011 - Energy Management Systems

Although OHSAS 18001:2007, ISO 28000:2007 and ISO 50001:2011 adopted the same structure as ISO 14001:2004, it differed from the structure of the following, most prevalent, MS standard. (Refer to Appendix 3.)

ISO 9001:2008 - Quality Management Systems [A very minor revision of ISO 9001:2000.]

These two structures also differed from that of the following MS standard. (Refer to Appendix 4.)

ISO 27001:2005 - Information Security Management Systems

This MS standard became increasingly adopted, and achieved strong growth in the number of certifications, because it addressed a growing need for management of an aspect of operations that now poses an increasing challenge to commercial organisations, governments and the military.

These standards all had common components, such as document and record control, internal audit, control of nonconformity, and management review etc., but with different clause numbers within each document. Consequently, these standards required cross reference tables, to show which clauses of each standard corresponded to equivalent clauses of other standards, to assist an organisation that wanted, or had to, implement two or more MS standards. Furthermore, there were other, increasingly adopted, MS standards, such as ISO 22000:2005 - Food Safety Management Systems and ISO/IEC 20000-1:2005 - Information Technology Service Management Systems, each with their own, different, structure. Organisations were increasingly required to implement a MS certified to multiple standards. It became obvious that it would be much easier to do this if they all shared a common structure.

3 Section and Sub-Section Headings of the HLS

Browse to the following webpage.

http://isotc.iso.org/livelink/livelink/Open/17859835

It links to the following document.

ISO/IEC Directives Part 1 and Consolidated ISO Supplement - Annex SL

This is Annex SL, which stipulates how to compile a MS standard. Appendix 2 (of the Annex SL document) specifies the common core text of the HLS, which all MS standards must contain. It consists of the following sections and sub-sections, each with some basic text content, where XXX is the type of MS (such as Information Security, Business Continuity, Environmental and Quality etcetera). Appropriate headings and text are added to this template to create each MS standard.

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 Organizational 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

4 Significant Components and Features of the HLS

4.1 Strategy - Context of the Organisation and Risks & Opportunities

A common and useful business exercise is to do a STEEPLE (or PESTLE) analysis followed by a SWOT analysis. The purpose of a SWOT analysis is to devise strategies. (Refer to Appendix 1).

The HLS includes components that constitute an amended form of these two stages of analyses.

(1) Determine the context of the organisation, including interested parties and their interests, which are relevant to the aspect of operations that the MS governs.

(a) The determination of the context requires an organisation to determine external and internal issues that are relevant to the aspects of operations that the MS governs.

(i) Do a STEEPLE (or PESTLE) analysis to identify external issues.

(ii) The determination of internal issues corresponds to the identification and assessment of Strengths and Weaknesses of a SWOT Analysis.

(b) The HLS requires an organisation to identify the Interested Parties (Stakeholders), and the interests (stakes) of these Interested Parties, with respect to the MS.

This is an implicit part of the STEEPLE (or PESTLE) and SWOT analyses.

An entity could be an interested party with respect to one MS, but not to another.

***Example** - A family living near a chemical processing plant would be an interested party with an interest in its Environmental Management System (EMS) but would not be an interested party with an interest in its Quality Management System (QMS).*

(2) Consider the risks and opportunities that arise from the context and interested parties.

The HLS requires an organisation to consider Risks and Opportunities.

The SWOT Analysis considers Strengths and Weaknesses (which are mostly internal factors), and Opportunities and Threats (which are mostly external factors).

(a) **Risks** - A Risk is the combination of an (external) Threat that the organisation cannot control, and an associated (internal) Vulnerabiliy that the organisation can control.

***Example** (Anti-Bribery) - **Threat** is an attempt to raise a false purchase order for a fictitious service. **Vulnerability** is the process to raise and authorise a purchase order. **Countermeasures** include: (i) due diligence checks on third parties, (ii) financial controls and (iii) non-financial controls.*

(b) **Opportunities** - An Opportunity is something that you can choose to pursue that has at least one associated possibility of a positive outcome.

The HLS requires MS standards to address Risks and Opportunities. It provides a definition of risk and specifies that risk can be negative or positive (i.e. the possibility of a negative or positive outcome). Unfortunately it does not explain positive risk or provide a definition of Opportunity. This has had the consequence that some guidance erroneously equates opportunity to positive risk, which is wrong. A risk is something that you are subject to, without choice. You may be subject to one or more, negative and/or positive, risks, after you choose to pursue an opportunity.

> ***Example*** *- The sale of lottery tickets provides an opportunity, to buy a lottery ticket. If you choose to buy a lottery ticket, you pursue an opportunity. This opportunity has an associated possibility of a positive outcome and an associated possibility of a negative outcome. The possibility of a positive outcome is that you win the lottery. This has a very low likelihood. The possibility of a negative outcome is that you lose your stake, i.e. the price of the ticket. This has a very high likelihood.*

The following document describes how to administer Opportunities and Risks.

http://www.parola.co.uk/MS/Annex_SL_HLS_-_Opportunities_and_Risks_-_Guide.pdf

WHAT and **HOW**	Before the application of the HLS, a MS standard required an organisation to know **WHAT** actions it does and **HOW** it does them, to effectively manage an aspect of operations, such as quality or information security.
WHY	A MS standard based on the HLS also now requires an organisation to know **WHY** it does those actions, to provide the foundation for **WHAT** and **HOW**.

4.2 Leadership

ISO 14001:2004, OHSAS 18001:2007 and ISO 28000:2007 contain several specific requirements of management in various parts of the standards. ISO 50001:2011 adds to the structure the additional sub-section ***4.2 - Management responsibility***. This corresponds to section ***5 - Management Responsibility***, starting with section ***5.1 - Management Commitment***, in both ISO 9001:2008 and ISO/IEC 27001:2005.

The HLS contains section ***5 - Leadership***, starting with section ***5.1 - Leadership and Commitment***.

> The use of the word **Leadership** instead of **Management** reinforces the two requirements to (i) identify the Context of the Organisation and (ii) address Risks and Opportunities.
>
> MS standards based on the HLS require the top management of an organisation to **LEAD** in addition to **MANAGE**.

4.3 Plan-Do-Check-Act (PDCA) Cycle

Seven of the ten main sections of the HLS correspond to stages of the **Plan-Do-Check-Act** cycle as follows.

Plan 4 – Context of the organization
5 – Leadership
6 – Planning

Do 7 – Support
8 – Operation

Check 9 – Performance evaluation

Act 10 – Improvement

The HLS provides better correspondence compared to that of superseded standards. For example, in both of ISO 14001:2004 and OHSAS 18001:2007, ***Section 4.4.1 – Resources, roles, responsibility (accountability and) authority*** is part of planning and would be better under ***Section 4.3 Planning*** than ***Section 4.4 Implementation and operation***.

Appendix 1
SWOT Analysis

A SWOT (*Strengths*, *Weaknesses*, *Opportunities* and *Threats*) Analysis applies to an organisation or enterprise. It provides a simple method to assist you to identify and assess, actual and potential, threats and opportunities, and to devise and select appropriate strategies to respond to them. You may wish to do a STEEPLE (*Social, Technological, Economic, Environmental, Political, Legal, Ethical*) [or PESTLE (*Political, Economic, Social, Technological, Legal, Environmental*)] Analysis before you do a SWOT Analysis. A STEEPLE (or PESTLE) Analysis applies to an operating environment or market, with respect to an organisation, enterprise, product or service. It provides a simple structured method to assist you to identify characteristic factors of the environment or market, including opportunities and threats. You use external threats and opportunities that you identify through a STEEPLE (or PESTLE) Analysis as inputs to a SWOT Analysis.

To do a SWOT Analysis, complete a SWOT Matrix, as shown below.

	Strengths *(1)* *(2)*	***Weaknesses*** *(1)* *(2)*
Opportunities *(1)* *(2)*	**S-O Strategies** (1) (2)	**W-O Strategies** (1) (2)
Threats *(1)* *(2)*	**S-T Strategies** (1) (2)	**W-T Strategies** (1) (2)

(1) Identify Strengths, Weaknesses, Opportunities and Threats.

IMPORTANT	(a)	*Strengths* and *Weaknesses* are internal aspects of the organisation.
	(b)	An aspect of the organisation may be a *Strength* and/or a *Weakness* in different circumstances.
	(c)	*Opportunities* and *Threats* are usually aspects of the (external) environment in which the organisation operates, but may be aspects of the environment within the organisation.
	(d)	*Opportunity* is NOT the opposite of *Threat*. An *Opportunity* is something that you can choose to pursue. An actual (not potential) *Threat* is something to which you are subject, without choice.
	(e)	An *Opportunity* may possess associated potential *Strengths*, *Weaknesses* and *Threats* which you will introduce if you choose to pursue the *Opportunity*.

(2) Devise the following four categories of strategies.

S-O Use *Strengths* to pursue *Opportunities*.
W-O Mitigate *Weaknesses* to pursue *Opportunities*.
S-T Use *Strengths* to mitigate susceptibility to *Threats*.
W-T Mitigate *Weaknesses* that increase susceptibility to *Threats* or avoid combinations of *Weaknesses* that increase susceptibility to *Threats*.

Appendix 2

ISO 14001:2004

1 Scope

2 Normative references

3 Terms and definitions

4 Environmental management system requirements

- 4.1 General requirements
- 4.2 Environmental policy
- 4.3 Planning
  - 4.3.1 Environmental aspects
  - 4.3.2 Legal and other requirements
  - 4.3.3 Objectives, targets and programme(s)
- 4.4 Implementation and operation
  - 4.4.1 Resources, roles, responsibility and authority
  - 4.4.2 Competence, training and awareness
  - 4.4.3 Communication
  - 4.4.4 Documentation
  - 4.4.5 Control of documents
  - 4.4.6 Operational control
  - 4.4.7 Emergency preparedness and response
- 4.5 Checking
  - 4.5.1 Monitoring and measurement
  - 4.5.2 Evaluation of compliance
  - 4.5.3 Nonconformity, corrective action and preventive action
  - 4.5.4 Control of records
  - 4.5.5 Internal audit
- 4.6 Management review

OHSAS 18001:2007

1 Scope

2 Reference publications

3 Terms and definitions

4 OH&S management system requirements

- 4.1 General requirements
- 4.2 OH&S policy
- 4.3 Planning
  - 4.3.1 Hazard identification, risk assessment and determining controls
  - 4.3.2 Legal and other requirements
  - 4.3.3 Objectives and programme(s)
- 4.4 Implementation and operation
  - 4.4.1 Resources, roles, responsibility, accountability and authority
  - 4.4.2 Competence, training and awareness
  - 4.4.3 Communication, participation and consultation
    - 4.4.3.1 Communication
    - 4.4.3.2 Participation and consultation
  - 4.4.4 Documentation
  - 4.4.5 Control of documents
  - 4.4.6 Operational control
  - 4.4.7 Emergency preparedness and response
- 4.5 Checking
  - 4.5.1 Performance measurement and monitoring
  - 4.5.2 Evaluation of compliance
  - 4.5.3 Incident investigation, nonconformity, corrective action and preventive action
    - 4.5.3.1 Incident investigation
    - 4.5.3.2 Nonconformity, corrective action and preventive action
  - 4.5.4 Control of records
  - 4.5.5 Internal audit
- 4.6 Management review

ISO 28000:2007

1 Scope

2 Normative references

3 Terms and definitions

4 Security management system elements

- 4.1 General requirements
- 4.2 Security management policy
- 4.3 Security risk assessment and planning
  - 4.3.1 Security risk assessment
  - 4.3.2 Legal, statutory and other security regulatory requirements
  - 4.3.3 Security management objectives
  - 4.3.4 Security management targets
  - 4.3.5 Security management programmes
- 4.4 Implementation and operation
  - 4.4.1 Structure, authority and responsibilities for security management
  - 4.4.2 Competence, training and awareness
  - 4.4.3 Communication
  - 4.4.4 Documentation
  - 4.4.5 Document and data control
  - 4.4.6 Operational Control
  - 4.4.7 Emergency preparedness, response and security recovery
- 4.5 Checking and corrective action
  - 4.5.1 Security performance measurement and monitoring
  - 4.5.2 System evaluation
  - 4.5.3 Security-related failures, incidents, non-conformances and corrective and preventive action
  - 4.5.4 Control of records
  - 4.5.5 Audit
- 4.6 Management review and continual improvement

ISO 50001:2011

1 Scope

2 Normative references

3 Terms and definitions

4 Energy management system requirements

- 4.1 General requirements
- 4.2 Management responsibility
  - 4.2.1 Top management
  - 4.2.2 Management representative
- 4.3 Energy policy
- 4.4 Energy planning
  - 4.4.1 General
  - 4.4.2 Legal requirements and other requirements
  - 4.4.3 Energy review
  - 4.4.4 Energy baseline
  - 4.4.5 Energy performance indicators
  - 4.4.6 Energy objectives, energy targets and energy management action plans
- 4.5 Implementation and operation
  - 4.5.1 General
  - 4.5.2 Competence, training and awareness
  - 4.5.3 Communication
  - 4.5.4 Documentation
  - 4.5.5 Operational control
  - 4.5.6 Design
  - 4.5.7 Procurement of energy services, products, equipment and energy
- 4.6 Checking
  - 4.6.1 Monitoring, measurement and analysis
  - 4.6.2 Evaluation of compliance with legal requirements and other requirements
  - 4.6.3 Internal audit of the EnMS
  - 4.6.4 Nonconformities, correction, corrective action and preventive action
  - 4.6.5 Control of records
- 4.7 Management review
  - 4.7.1 General
  - 4.7.2 Input to management review
  - 4.7.3 Output from management review

Appendix 3
ISO 9001:2008

1 Scope
- 1.1 General
- 1.2 Application

2 Normative references

3 Terms and definitions

4 Quality management system
- 4.1 General requirements
- 4.2 Documentation requirements
  - 4.2.1 General
  - 4.2.2 Quality manual
  - 4.2.3 Control of documents
  - 4.2.4 Control of records

5 Management responsibility
- 5.1 Management commitment
- 5.2 Customer focus
- 5.3 Quality policy
- 5.4 Planning
  - 5.4.1 Quality objectives
  - 5.4.2 Quality management system planning
- 5.5 Responsibility, authority and communication
  - 5.5.1 Responsibility and authority
  - 5.5.2 Management representative
  - 5.5.3 Internal communication
- 5.6 Management review
  - 5.6.1 General
  - 5.6.2 Review input
  - 5.6.3 Review output

6 Resource management
- 6.1 Provision of resources
- 6.2 Human resources
  - 6.2.1 General
  - 6.2.2 Competence, training and awareness
- 6.3 Infrastructure
- 6.4 Work environment

7 Product realization
- 7.1 Planning of product realization
- 7.2 Customer-related processes
  - 7.2.1 Determination of requirements related to the product
  - 7.2.2 Review of requirements related to the product
  - 7.2.3 Customer communication
- 7.3 Design and development
  - 7.3.1 Design and development planning
  - 7.3.2 Design and development inputs
  - 7.3.3 Design and development outputs
  - 7.3.4 Design and development review
  - 7.3.5 Design and development verification
  - 7.3.6 Design and development validation
  - 7.3.7 Control of design and development changes
- 7.4 Purchasing
  - 7.4.1 Purchasing process
  - 7.4.2 Purchasing information
  - 7.4.3 Verification of purchased product
- 7.5 Production and service provision
  - 7.5.1 Control of production and service provision
  - 7.5.2 Validation of processes for production and service provision
  - 7.5.3 Identification and traceability
  - 7.5.4 Customer property
  - 7.5.5 Preservation of product
- 7.6 Control of monitoring and measuring equipment

8 Measurement, analysis and improvement
- 8.1 General
- 8.2 Monitoring and measurement
  - 8.2.1 Customer satisfaction
  - 8.2.2 Internal audit
  - 8.2.3 Monitoring and measurement of processes
  - 8.2.4 Monitoring and measurement of product
- 8.3 Control of nonconforming product
- 8.4 Analysis of data
- 8.5 Improvement
  - 8.5.1 Continual improvement
  - 8.5.2 Corrective action
  - 8.5.3 Preventive action

Appendix 4

ISO 27001:2005

1 Scope

1.1 General

1.2 Application

2 Normative references

3 Terms and definitions

4 Information security management system

4.1 General requirements

4.2 Establishing and managing the ISMS

4.2.1 Establish the ISMS
4.2.2 Implement and operate the ISMS
4.2.3 Monitor and review the ISMS
4.2.4 Maintain and improve the ISMS

4.3 Documentation requirements

4.3.1 General
4.3.2 Control of documents
4.3.3 Control of records

5 Management responsibility

5.1 Management commitment

5.2 Resource management

5.2.1 Provision of resources
5.2.2 Training, awareness and competence

6 Internal ISMS audits

7 Management review of the ISMS

7.1 General

7.2 Review input

7.3 Review output

8 ISMS improvement

8.1 Continual improvement

8.2 Corrective action

8.3 Preventive action