Five Ways to Integrate
Management System Standards

Most ISO Management System (MS) standards share a common structure, originally known as the High Level Structure (HLS), published in December 2012. This is specified in Annex SL, which is part of a large ISO specification document. A (minor) revision was published in May 2021 and it is now known as the Harmonised Structure (HS). This common structure facilitates the implementation of an Integrated Management System (IMS), when an organisation must implement two or more MSSs. If the MSSs apply to disparate activities or aspects of operations, such as information security and environmental impact, the HLS eases integration, because components common to all MSSs have identical or similar clause numbers in the different standards.

However, some MSSs contain requirements that enable or require, additional, more fundamental and inherent integration between two or more MSSs, as follows.

1 Annex SL, High Level Structure (HLS)

A management system that implements two or more management system standards can, at the least, combine common equivalent components, such as the following, of the Annex SL, HLS framework.

(1) Determine processes.

(2) Determine external issues.
Determine internal issues.

(3) Determine interested parties and their interests with respect to the organisation.
Determine the organisation's interests with respect to the interested parties.

(4) Determine opportunities and risks.
Determine organisation's strategy.

(5) Internal Audits.

(6) Management Review.

2 Complementary Combinations of Standards

It may be appropriate to implement multiple standards to more effectively manage different aspects of products and services, as in the following examples.

(1) ISO 41001 – Facility Management System

ISO 50001 – Energy Management System

Facilities management is the provision of buildings and services, for commercial, industrial and residential use. Modern buildings are increasingly designed to be energy efficient and the energy efficiency of older buildings can be improved by double or triple glazed windows and effective (loft and/or cavity wall) insulation.

(2) ISO 41001 – Facility Management System

ISO 20000-1 – Information Technology Service Management System

It is increasingly common for commercial rental properties for small businesses to also offer ICT services (computer networking, internet access and telephony etcetera).

3 Standards with Common Risks, Opportunities and/or Objectives

An organisation's Risks, Opportunities or Objectives may relate to two or more aspects of operation as in the following examples.

(1) ISO 50001 – Energy Management System

ISO 14001 – Environmental Management System

If an organisation manages its energy consumption, it will invariably also influence its environmental impact.

(2) ISO 41001 – Facility Management System

ISO 45001 – Occupational Health and Safety Management System

An entity that provides facilities must ensure that the facilities are inherently safe.

(3) ISO 37001 – Anti-Bribery Management System

ISO 9001 – Quality Management System

If the award of a contract is not corruptly influenced by bribery, it is more likely that the contract will be awarded to the organisation that can deliver the optimum quality (and/or value) of products and/or services.

(4) ISO 37001 – Anti-Bribery Management System

ISO 55001 – Asset Management System

ISO 55001 manages the value of an organisation's (tangible and intangible) assets. Many companies now purposely cultivate an ethical culture and social responsibility, to appeal to increasingly discerning customers. Consequently, a company's brand and reputation can be valuable intangible assets. Conversely, a company's brand and reputation are invariably significantly devalued by any allegations of corruption.

4 Standards that Address Requirements of other Standards

One management system standard may apply to an activity or aspect of operations that addresses a requirement of another standard as in the following examples.

(1) ISO/IEC 27001 addresses requirements of the following.

(a) ISO/IEC 20000-1, Clause 8.7.3 – Information security management

(b) ISO 37001, Clause 8.3 – Financial controls and Clause 8.4 – Non-financial controls

ISO 37001, Clauses 8.3 and 8.4 both only specify that the organisation must operate *Financial controls* and *Non-financial controls*. (Annex A provides guidance in Clauses A.11 – Financial controls and A.12 – Non-financial controls.) The organisation must manage, and maintain adequate records of, its activities, expenditure and income.

The organisation must ensure the Integrity (completeness and accuracy), Availability and Confidentiality of the financial and non-financial records of its activities. This is Information Security.

(2) ISO 22301 addresses requirements of the following.

(a) ISO/IEC 27001, Control A.17.1 – Information security continuity

(b) ISO 41001, Clause 6.1 – Actions to address risks and opportunities

– ensure business continuity and emergency preparedness.

(3) ISO 41001 addresses a requirement of the following.

(a) ISO 21001 – Management System for Educational Organizations, Clause 7.1.3 – Facilities

5 Standards with Mechanisms that can Reinforce other Standards

One management system standard may contain a requirement for a mechanism that can be usefully applied to reinforce one or more (or potentially all) other standards, as in the following examples.

(1) ISO 9001, Clause 4.4 – Processes

All management system standards (based on the HLS) require you to identify the processes that the management system requires. ISO 9001, Clause 4.4.1 specifies a number of requirements, including the following, which should be should be done for all essential business processes, and additional processes to manage other activities or aspects of operations (e.g. information security for ISO/IEC 27001, anti-bribery for ISO 37001 etcetera).

(a) Determine the processes that the (integrated) management system requires.

(b) Determine the sequence and interaction of the processes.

(c) Determine the inputs that each process requires.

(d) Determine the outputs expected from each process.

(e) Determine the resources that each process requires and ensure that they are available.

(f) Assign responsibilities and authorities for each process.

(g) Address risks and opportunities associated with the processes.

(2) ISO 37001, Clause 5.1.1 and Clause 9.3.2 – Governing Body

Other management system standards require leadership and support from the (operational) Top Management, as does ISO 37001, Clause 5.1.2.

However, if an organisation has a Governing Body:

Clause 5.1.1 requires the Governing Body to approve and oversee the Anti-bribery management system;

Clause 9.3.2 requires the Governing Body to review the Anti-bribery management system.

An (integrated) management system that complies with ISO 37001, together with one or more other management system standards, such as ISO/IEC 27001, can be implemented so that other components, in addition to its anti-bribery components, require the approval and oversight of the Governing Body.

(3) ISO 45001, Clause 5.4 – Consultation and participation of workers

This clause is essential for effective management of occupational health and safety.

– To ensure the safety of its workers, an organisation must make decisions about, how workers do their work, what equipment they must use, what clothing they must wear and what training they must receive.

– The organisation must consult workers to ensure that the organisation has access to all the required information to make the decisions.

– Workers must participate in those decisions to ensure that they accept and support the decisions.

Formal consultation and participation of workers may be beneficial for management of other aspects of operations such as ISO 9001 – Quality Management. It would NOT be substantially beneficial for management of an aspect of operations that requires specific knowledge or skills, such as ISO 55001 – Asset Management.

(4) ISO/IEC 27001 Controls

ISO 37001

ISO/IEC 27001, Control A.8.2 – Classification of information

This control specifies requirements to classify information (for example as Public, Unrestricted, Restricted, Confidential, Sensitive, Secret etcetera), and define how you label and handle information with different classifications.

It can formalise the control of documentation to reinforce the following clauses of ISO 37001:

Clause 7.5 – Documented information;

Clause 8.9 – Raising concerns;

Clause 8.10 – Investigating and dealing with bribery.

ISO 44001

ISO/IEC 27001, Control A.8.2 – Classification of information
and
ISO/IEC 27001, Control A.13.2 – Information transfer

The second of these controls specifies requirements to ensure that an organisation securely transfers information, both internally, and externally to/from other entities.

These can formalise the control of documentation to reinforce the following clauses of ISO 44001:

Clause 8.3.4 – Knowledge management;

Clause 8.6.2 – Joint management arrangements, Item 5;

Clause 8.6.3 – Joint knowledge management process;

Clause 8.6.5 – Operational process and systems review, Item 6.

(5) ISO 37301, Clauses 3.27 – Noncompliance and 10.2 – Nonconformity and corrective action

One component of all management system standards is a Nonconformity (the non-fulfilment of a requirement). When a Nonconformity is revealed, it is necessary to determine its Root Cause and decide upon a Corrective Action, to prevent its recurrence. Some management system standards have their own individual variations or manifestations of this that require Corrective Action. For example, ISO 9001 has a Customer Complaint and ISO/IEC 27001 has an Information Security Incident. ISO 37301 has a Noncompliance.

Several other management system standards require an organisation to identify applicable legal and regulatory requirements and detail how the management system complies with them, including ISO 14001, ISO 22301, ISO 37001, ISO 39001, ISO 45001, ISO 50001, ISO 55001, ISO/IEC 27001 and ISO/IEC 27701.

It is useful to add Noncompliance to the possible categories [Nonconformity, (Information Security) Incident, Accident etcetera] that you use to categorise issues in a management system.

For example, a data breach could be categorised as a Nonconformity, an Information Security Incident and a Noncompliance.