Different Implementations of Risk Management

Until 2005 there were two (significant) international management system standards, ISO 9001 - Quality Management Systems and ISO 14001 - Environmental Management Systems. Then ISO and IEC published ISO/IEC 27001 - Information Security Management Systems. There are now many more management system standards, almost all of which now have a common structure. This was originally the High Level Structure (HLS), published in December 2012. A (minor) revision was published in May 2021 and it is now known as the Harmonised Structure (HS). The HS is a set of common clause numbers, headings and core text that all management system standards must contain, as specified in Appendix 2 of Annex SL.

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

https://isotc.iso.org/livelink/livelink/fetch/-8921878/8921901/16347356/16347818/2021-05_Annex_SL_Appendix_2.pdf

https://isotc.iso.org/livelink/livelink/fetch/-8921878/8921901/16347356/16347818/2021-05_Annex_SL_Appendix_3.pdf

As the number of management system standards that manage different aspects of operations increases, there is an increasing need to be able to implement an Integrated Management System (IMS) that encompasses and conforms to multiple management system standards.

Unaligned Implementations of Risk Management

(A) The HS contains a requirement to address {strategic} risks and opportunities that relate to the effectiveness of the management system, to determine strategy.

(B) The HS does NOT contain a requirement for a formal risk assessment (maintenance of a risk register) of {operational} risks that a management system must manage.

Unfortunately, different management system standards specify requirements for risk management that do not conveniently align. They differ in detail, and appear in different clauses of various standards. Moreover, some also confuse the distinction between {strategic} risks to the effectiveness of the management system and {operational} risks that the management system must manage.

To implement an Integrated Management System (IMS) that conforms to multiple management system standards, you should be aware of the different nature and details of the different implementations of risk management in the individual management system standards.

Annex SL Harmonised Structure (HS) Guidance

Appendix 2 of Annex SL" specifies the headings and core text of the HS, and also explains the intent and purpose of all clauses of the HS.

https://isotc.iso.org/livelink/livelink/fetch/-8921878/8921901/16347356/16347818/2021-05_Annex_SL_Appendix_2.pdf

This explains that the intention of Clause **6.1 Actions to address risks and opportunities** in the HS is to perform planning to establish the management system.

Clause 6.1 refers to risks and opportunities that relate to the effectiveness of the management system; it does not refer to risks that the management system must manage, such as risks of disruption of business activities. The intended purpose of Clause 6.1 is to devise STRATEGY.

The guidance assumes that {strategic} risks to the effectiveness of the management system and {operational} risks that the management system must manage are separate. However, for some aspects of operations, such as information security and bribery, identified operational risks may substantially affect the implementation of the management system.

Details of the Different Implementations of Risk Management

ISO 22301:2019 - Business Continuity Management Systems

(1) This standard puts risk management in Clause **8.2**. It contains the following two notes, at the ends of Clauses **6.1** and **8.2**, which clearly distinguish the purposes of the two clauses.

> ***6.1 Actions to address risks and opportunities***
>
> *NOTE Risks and opportunities relate to the effectiveness of the management system. Risks related to disruption of the business are addressed in 8.2.*
>
> ***8.2 Business impact analysis and risk assessment***
> ***8.2.3 Risk assessment***
>
> *NOTE Risks in this subclause relate to the disruption of business activities. Risks and opportunities related to the effectiveness of the management system are addressed in 6.1.*

(2) The standard puts the management of operational risks in Clause 8.

ISO/IEC 27001:2013 - Information Security Management Systems

(1) This standard specifies the requirement to address risks and opportunities related to the effectiveness of the management system in Clause **6.1.1 General**.

(2) This is followed by requirements for the ***methodology*** of assessment and treatment of information security risks in Clauses **6.1.2 Information security risk assessment** and **6.1.3 Information security risk treatment**. The requirements to ***perform*** assessment and treatment of information security risks are in Clauses **8.2 - Information security risk assessment** and **8.3 Information security risk treatment**.

(3) This standard puts the management of operational risks in both Clauses 6 and 8.

(4) The inclusion of the requirements for the methodology of management of {operational} information security risks in Clause **6.1 Actions to address risks and opportunities** weakens the distinction between the requirement to address {strategic} risks and opportunities related to the effectiveness of the management system and the requirement to address {operational} information security risks.

ISO 45001:2018 - Occupational Health and Safety Management Systems

(1) This standard specifies the requirement to address risks and opportunities related to the effectiveness of the management system in Clause **6.1.1 General**, followed by requirements to identify hazards, and assess occupational health and safety risks and opportunities, in Clause **6.1.2 Hazard identification and assessment of risks and opportunities**.

(2) The combination of the two requirements together in Clause **6.1 Actions to address risks and opportunities** weakens the distinction between the requirement to address risks and opportunities related to the effectiveness of the management system and the requirement to address {operational} occupational health and safety risks.

(3) This standard puts the management of operational risks in Clause 6.

ISO 37001:2016 - Anti-Bribery Management Systems

(1) This standard specifies requirements to assess {operational} bribery risks in Clause **4.5 Bribery risk assessment**.

(2) This is separate from the requirement to address {strategic} risks and opportunities related to the effectiveness of the management system in Clause **6.1 Actions to address risks and opportunities**.

(3) Clause 4.5 ends with the requirement **4.5.4 The organization shall retain documented information that demonstrates that the bribery risk assessment has been conducted and used to design or improve the anti-bribery management system**. This wording at the end of Clause **4.5 Bribery risk assessment** weakens the distinction between the requirement to address {strategic} risks and opportunities related to the effectiveness of the management system and the requirement to address {operational} bribery risks.

(4) This standard puts the management of operational risks in Clause 4.

ISO 37301:2021 - Compliance Management Systems

(1) This standard specifies requirements to assess {operational} compliance risks in Clause **4.6 Compliance risk assessment**.

(2) This is separate from the requirement to address {strategic} risks and opportunities related to the effectiveness of the management system in Clause **6.1 Actions to address risks and opportunities**.

(3) This standard puts the management of operational risks in Clause 4.

Summary

ISO 22301 provides an unambiguous implementation of risk management, and clearly distinguishes between assessment of {strategic} risks and opportunities related to the effectiveness of the management system and {operational} risks that the management system must manage.

ISO 37301 provides an unambiguous implementation of risk management, and clearly distinguishes between assessment of {strategic} risks and opportunities related to the effectiveness of the management system and {operational} risks that the management system must manage.

ISO/IEC 27001, ISO 45001 and ISO 37001 provide definitive requirements for risk management but less explicitly distinguish between assessment of {strategic} risks and opportunities related to the effectiveness of the management system and {operational} risks that the management system must manage.

Conclusion

These management system standards all provide different specifications for implementation of risk assessment. However, they are all sufficiently similar that an organisation can implement an Integrated Management System (IMS) that conforms to any two or more standards, with:

(A) An integrated assessment of {strategic} risks and opportunities related to the effectiveness of the management system;

(B) An integrated assessment of {operational} risks that the management system must manage.