irm

Standard Deviations

A Risk Practitioners Guide to ISO 31000

2018

About IRM

IRM is the leading professional body for risk management. We are an independent, not-for-proft organisation that champions excellence in managing risk to improve organisational performance.

We do this by providing internationally recognised qualifcations and training, publishing research and guidance and raising professional standards across the world. Our members work in all industries, in all risk disciplines and across the public, private and not-for-proft sectors.

Registered Offce: 2nd Floor, Sackville House, 143-149
Fenchurch Street, London, EC3M 6BN

T – +44 (0)20 7709 9808
E – enquiries@theirm.org
W – www.theirm.org

Contents

1. Executive Summary

There are many recommended approaches to risk management (RM) and several different guides and risk management frameworks and standards have been published. This guide explains the approach used in ISO 31000:2018 *Risk management – Guidelines* and identifies the importance and relevance of ISO 31000 and other frameworks. This guide also outlines the practical application of the ISO 31000 guidelines and provides commentary on implementation.

It remains a challenge for risk professionals to clearly demonstrate the value of making resources available for risk management. In view of this continuing challenge, ISO has published an updated version of ISO 31000 *Risk management – Guidelines*. This IRM guide provides commentary on the revised ISO 31000. In 2017 COSO published '*ERM – Integrating Strategy and Performance*' and a separate IRM guide to the updated COSO framework has also been published.

In order to evaluate ISO 31000 and, in the separate guide, the updated COSO framework, a recognised format is necessary. The International Standards Organisation (ISO) published a highly regarded guide to the format for management system standards entitled Annex SL. The Annex SL format for management system standards is summarised in Appendix A of this guide.

Annex SL describes seven substantive components of a management system standard. These are grouped in this guide as 'Scope and Design' components and 'Control and Develop' components, as illustrated in Figure 1 and Figure 2, respectively. This guide considers these two groups of components as the means of comparing ISO 31000 with the Annex SL format. The conclusion is that ISO 31000 includes all the required features of a management system standard, but with the emphasis on the 'Control and Develop' components.

Overall, ISO 31000 provides detailed guidelines on the plan, implement, measure and learn features of a risk management system, but less explicit information on the context, leadership and support features required of a management system standard. An analysis of the components of ISO 31000 is provided in Appendix B. The message for risk professionals is that their employer or client organisations should implement the ISO 31000 principles and components that are best suited to their particular circumstances and modify other principles and components, as necessary.

ISO 31000 containes much valuable information and it represents robust, high-level guidelines for the management of risk. However, there is no step-by-step checklist to implementation of the risk management initiative. The challenge for risk professionals is to rearrange the guidance in ISO 31000 to align with their own approach to implementing a risk management initiative. This guide provides an analysis of ISO 31000, a comparison with the ISO format for management system standards (Annex SL) and outlines a checklist for the implementation of a risk management initiative in Section 9.

2. Nature of management systems

A management system is the framework of policies, processes and procedures employed by an organisation to ensure that it can fulfill the tasks required to achieve its purpose and objectives. These objectives will cover all aspects of the organisation, including strategy, tactics, operations and compliance. For instance, a quality management system enables organisations to improve the quality and consistency of products and/or services.

ISO has published a guide to management system standards with information on the sections that should be included. This ISO guidance is published as Annex SL and several standards have already been converted into this format. ISO 9001 on quality management is the best established international standard and was updated in 2015 using the Annex SL format. Several existing ISO management system standards are being converted into the Annex SL format, including ISO 14001 – *Environmental management systems* and ISO 45001 – *Occupational health and safety management systems*.

Given the well-established nature of Annex SL and the fact that ISO 9001 has already been converted into this format, it is the most appropriate structure against which to judge the completeness of ISO 31000. A summary of the Annex SL format is provided in Appendix A. However, ISO 31000 and the COSO framework *Enterprise Risk Management – Integrating with Strategy* are not in the Annex SL format. Table 2 in Section 8 of this guide compares ISO 31000 with the Annex SL format and provides a useful means of testing the completeness of ISO 31000.

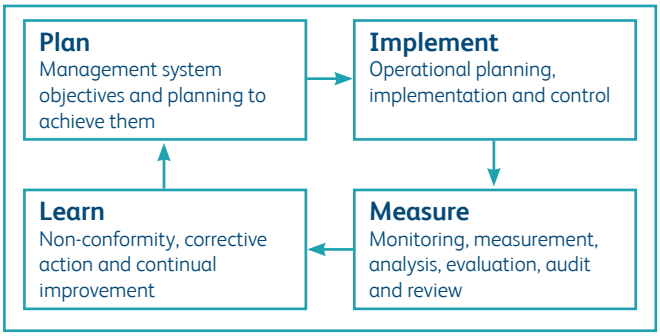
In order to review ISO 31000, the Annex SL components have been grouped into components that consider the 'Scope and Design' and components that consider the 'Control and Develop' features of a management system. The Annex SL components relevant to 'Scope and Design' are context, leadership and support. The components relevant to 'Control and Develop' are planning, operation, performance and improvement. These latter components are equivalent to plan, implement, measure and learn (PIML) or the plan-do-check-act approach used in some management systems.

Figure 1 illustrates the relationship between the three components of the 'Scope and Design' and Figure 2 illustrates the relationship between the four components of 'Control and Develop'. Presentation of the Annex SL components in this format separates the 'Scope and Design' components, which represent the framework for supporting risk management from the 'Control and Develop' components which represent the risk management process itself.

Formalised management systems have defined, documented processes that are intended to explicitly manage processes within an organisation. These will be auditable standards developed for each activity or process. Informal management systems are implicit and may include roles and responsibilities, audits and management of change. However, for larger organisations formalised processes are essential and that explains the importance of published standards, such as ISO 9001 and ISO 31000.

Figure 1: Scope and design components of management systems

Figure 2: Control and develop components of management systems



3. Changing risk context for organisations

The World Economic Forum (WEF) has commented on the increasing volatility, uncertainty, complexity and ambiguity of the world. WEF states that the current competitive landscape can be defined by one word: 'disruption'. WEF states that the ideas of incremental progress, continuous improvement, and process optimizations do not work anymore. WEF acknowledges that these practices are necessary, but are insufficient.

WEF supports the analysis that stakeholders are more engaged today, seeking greater transparency and accountability for managing the impact of risk, while also critically evaluating leadership ability to embrace opportunities. Even success can bring with it additional downside risk, such as the risk of not being able to fulfill unexpectedly high demand or maintain expected business momentum. Organisations and board members need to be more adaptive to change. They need to think strategically about how to manage the increasing volatility, uncertainty, complexity and ambiguity of the world.

Following the global financial crisis in 2008, all organisations are taking a greater interest in risk and risk management. It is increasingly understood that the explicit and structured management of risk brings benefits. By taking a proactive approach to risk and risk management, organisations will be able to achieve the following four areas of improvement:

- Strategy, because the risks associated with different strategic options will be fully analysed and better strategic decisions will be reached.
- Tactics, because consideration will have been given to selection of the tactics and the risks involved in the alternatives that are available.
- Operations, because events that can cause disruption will be identified and actions taken to reduce the likelihood of these events, limit the damage and contain the cost.
- Compliance will be enhanced because the risks associated with failure to achieve compliance with statutory and customer obligations will be recognized.

Indeed, it is no longer acceptable for organisations to find themselves in a position whereby unexpected events cause financial loss, disruption to normal operations, damage to reputation and loss of market presence. Stakeholders now expect that organisations will take full account of the risks that may cause non-compliance with statutory obligations; disruption and inefficiency within operations; late delivery of projects; or failure to deliver promised strategy.

There are an increasing number of risks faced by organisations. Some of these risks relate to managing the organisation and others relate to rapid and/or unexpected changes in the marketplace. Most organisations need to manage risks associated with:

- Variable cost or availability of raw materials.
- Cost of retirement/pension/social benefits.
- Increasing importance of intellectual property (IP).
- Greater supply chain and joint venture dependency and complexity.
- Reputation becoming more important and more vulnerable.
- Regulatory pressures and legislative requirements increasing.

The changes in the marketplace can be even more dramatic and include:

- Volatile markets and globalization of customers, suppliers and products.
- Increased competition in the marketplace and greater customer expectations.
- Product innovation and rapid changes in product technology.
- Threats to national economies and restricted freedom of world trade.
- Potential for international organised crime and increased political risks.
- Extreme weather events resulting in destruction and/or population shift.

Management holds overall responsibility for managing risks to the organisation, but it is important for senior management to go further and enhance the conversation with the board and stakeholders. Risk management needs to be used to gain a competitive advantage. Through enhanced risk management, senior management and the board will gain a better understanding of how the explicit consideration of risk may beneficially impact the choice of strategy.

Traditionally, risk management has played a strong supporting role at board level. Now, boards are increasingly expected to provide robust oversight of risk management. ISO 31000 provides important information for boards, so that they can define and fulfil their risk oversight responsibilities. These considerations include governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the review and revision of practices to enhance the performance of the organisation.

However, there is a danger when implementing ISO 31000 that the output from the risk management process forms a stream of management information that is separate from the other information required to successfully manage the organisation. It is important that risk managers undertake their activities in a way that aligns with the current business model and the strategy for the future.

Integrating consideration of risk into existing management activities will ensure that risk information is part of the management information used by executives and board members. This will help overcome the perception that risk management is only concerned with compiling and managing a list of risks and this can be undertaken separately from the day-to-day management of the organisation and the development of strategy for the future.

4. Structure and approach of ISO 31000

ISO 31000 was originally published in 2009 and an updated version was published in February 2018. However, the overall purpose of ISO 31000 remains the same – integrating the management of risk into a strategic and operational management system. The 2018 version is very similar to the original version, but the following bullet points identify the main changes for the 2018 version of the guidelines:

- the principles of risk management have been reviewed, as these are the key criteria for successful risk management;
- the importance of leadership by top management is highlighted, as is the integration of risk management, starting with the governance of the organisation;
- greater emphasis is placed on the iterative nature of risk management, because new knowledge and analysis leads to revision of processes, actions and controls; and
- the content is streamlined with greater focus on sustaining an open systems model to fit multiple needs and contexts.

ISO 31000:2018 *Risk Management – Guidelines*

A lot of the complicated language has been eliminated, so the text is leaner and more precise. The new draft is shorter, but it gains in clarity and precision and is much easier to read. It includes improvements, such as the importance of human and cultural factors in achieving an organisation's objectives and an emphasis on embedding risk management within the decision-making process.

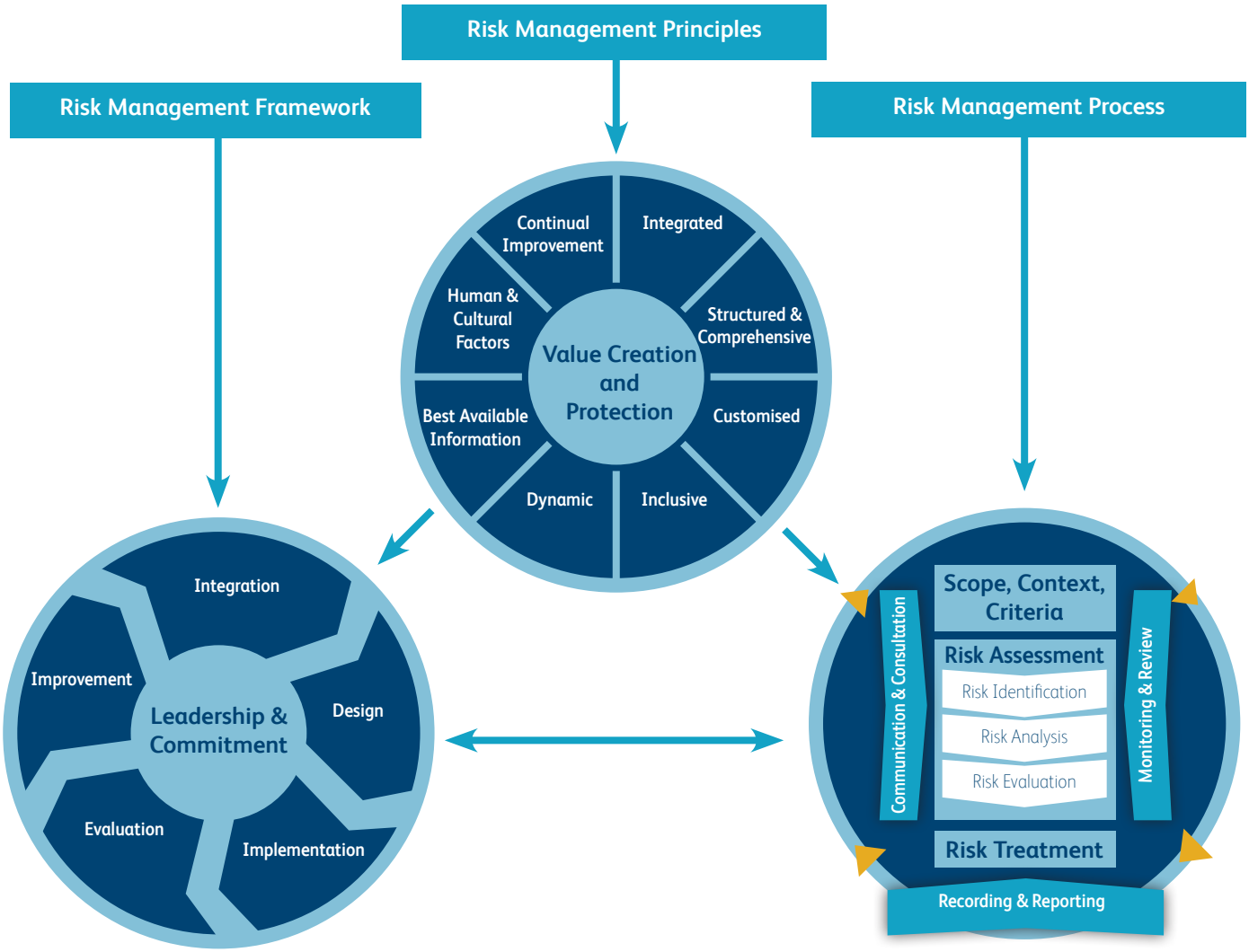
Edited extract from ISO website, www.iso.org

As with all ISO standards and guidelines, the first substantive section defines key terms. A total of eight terms are defined, including the definition of risk as "the effect of uncertainty on objectives". This definition is clarified by a note to the definition stating that risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

The new version of ISO 31000 is shorter than the earlier version, and it presents a high-level overview of risk management and how a risk management initiative can be implemented. ISO 31000 suggests that effective risk management is characterised by principles, framework and process. The separation of principles, framework and process is not in line with the suggested format for management system standards, as described in Annex SL. This may present the risk professional with a challenge when seeking to produce an implementation plan or checklist for their risk management initiative based on ISO 31000.

The overall structure and approach adopted by the 2018 edition of ISO 31000 is best illustrated by the diagram included in ISO 31000 and reproduced over the page as Figure 3. ISO 31000 states that managing risk is based on the principles, framework and process described in the guidelines. It also states that these principles and components might already exist in full or in part within an organisation, but they might need to be adapted or improved so that managing risk is efficient, effective and consistent.

Figure 3: Principles, framework and risk management process from ISO 31000



ISO 31000 states that the guidelines should be used by people who create and protect value in organisations by managing risks, making decisions, setting and achieving objectives and improving performance. The guidelines are applicable to all types and sizes of organisations and relevant to all external and internal factors and influences. They also state that managing risk assists organisations in setting strategy, achieving objectives and making informed decisions. Managing risk is part of governance and leadership and is fundamental to how organisations are managed at all levels.

5. Guidance provided in ISO 31000 – principles

ISO 31000 states that the purpose of risk management is the creation and protection of value. The principles set out in ISO 31000 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. There are total of eight principles presented in the standard, as shown in Figure 3 of this guide.

The ISO 31000 guidelines provide a statement of risk management principles. The eight principles are described below:

1. Framework and processes should be customised and proportionate.
2. Appropriate and timely involvement of stakeholders is necessary.
3. Structured and comprehensive approach is required.
4. Risk management is an integral part of all organisational activities.
5. Risk management anticipates, detects, acknowledges and responds to changes.
6. Risk management explicitly considers any limitations of available information.
7. Human and cultural factors influence all aspects of risk management.
8. Risk management is continually improved through learning and experience.

The first five principles provide guidance on how a risk management initiative should be designed, and principles six, seven and eight relate to the operation of the risk management initiative. These latter principles confirm that the best information available should be used; human and cultural factors should be considered; and the risk management arrangements should ensure continual improvement.

The first five principles are concerned with the design and planning of the risk management initiative and these principles are often summarised as proportionate, aligned, comprehensive, embedded and dynamic (PACED), as shown in Table 1.

Table 1: Principles of risk management

Principle	Description
Proportionate	Risk management activities must be proportionate to the level of risk faced by the organisation.
Aligned	Risk management activities need to be aligned with the other activities in the organisation.
Comprehensive	In order to be fully effective, the risk management approach must be comprehensive.
Embedded	Risk management activities need to be embedded within the organisation.
Dynamic	Risk management activities must be dynamic and responsive to emerging and changing risks.

6. Guidance provided in ISO 31000 – framework

The principles of risk management and the framework are closely related. For example, one of the principles is that risk management should be integrated and one of the components of the framework is integration. The principle outlines what must be achieved, and the framework provides information on how to achieve the required integration.

The ISO 31000 guidelines are centered on leadership and commitment. The effectiveness of risk management will depend on its integration into all aspects of the organisation, including decision-making. The remaining components of the framework are design, implementation, evaluation and improvement. This approach is often represented in management literature as plan-do-check-act. It is similar to the plan, implement, measure learn (PIML) approach described in Section 9 of this guide.

ISO 31000 provides narrative description of how the framework should support risk management activities in an organisation. This is often referred to as the risk architecture, strategy and protocols of the organisation, as set out in Table 2. There is information in ISO 31000 about the extent of leadership and commitment that is required, and the range of activities involved in designing and implementing the risk management initiative, and this information is compatible with the activities listed in Table 2.

Table 2: Risk management framework

Risk management architecture

- Committee structure and terms of reference
- Roles and responsibilities
- Internal reporting requirements
- External reporting controls
- Risk management assurance arrangements

Risk management strategy

- Risk management philosophy
- Arrangements for embedding risk management
- Risk appetite and attitude to risk
- Benchmark tests for significance
- Specific risk statements/policies
- Risk assessment techniques
- Risk priorities for the present year

Risk management protocols

- Tools and techniques
- Risk classification system
- Risk assessment procedures
- Risk control rules and procedures
- Responding to incidents, issues and events
- Documentation and record keeping
- Training and communications
- Audit procedures and protocols
- Reporting/disclosures/certification

ISO 31000 places great emphasis on understanding the organisation and its context. Information is provided on how to examine both the external and internal context of the organisation. There is also advice and guidance on articulating risk management commitment, assigning roles and responsibilities and allocating resources. There is some guidance on establishing communication and consultation in the framework section of ISO 31000 with more detailed information in the process section of the guidelines. Therefore, the guidance on communication and consultation in the framework section needs to be read in conjunction with the guidance on the same topic in the process section of ISO 31000.

Understanding the organisation and its context is included as part of the framework guidance in ISO 31000 and is also included in the process section under the heading 'scope, context, criteria'. The components of establishing the context are described as defining the purpose and scope of risk management activities; establishing the external, internal and risk management context; and defining the risk criteria. Defining the risk criteria involves specifying the amount and type of risk that the organisation may or may not take, relative to objectives. This is usually referred to as the 'risk appetite' of the organisation.

However, ISO 31000 does not use the phrase 'risk appetite', even though it is defined in the ISO Guide 73:2009 *Risk management – Vocabulary*. Risk appetite is defined in Guide 73 as the amount and type of risk that an organisation is willing to pursue or retain. The phrase 'risk appetite' is used by many organisations and is frequently described in the annual report and accounts of a wide range of different types of organisation. ISO 31000 provides guidance on the concept of 'risk criteria', but no guidance specific to the more commonly used concept of 'risk appetite'.

7. Guidance provided in ISO 31000 – process

The section of ISO 31000 concerned with the risk management process describes risk assessment and risk treatment as being at the centre of the risk management process. This section also includes guidance on (1) scope, context and criteria; (2) communication and consultation; (3) monitoring and review; and (4) recording and reporting. In many organisations, these latter four related activities are more closely aligned with the framework. It could be argued that these four activities are part of the risk management context and, therefore, should be part of the risk management framework. The risk management framework is often described as the risk architecture, strategy and protocols of the organisation.

The nature and extent of risk management activities in an organisation are influenced by risk attitude and risk appetite. The risk attitude and risk appetite of the organisation, as supported by the risk criteria for different types of risks, helps to define the risk management context of the organisation. Risk attitude and risk appetite also provide the foundations for undertaking risk assessments and recording the results in the risk register. The nature and extent of communication of the information contained in the risk register throughout the risk architecture of the organisation also helps define the risk management context.

The risk management context is part of the internal context of an organisation. The internal context refers to the organisation itself, the activities it undertakes, the range of skills and capabilities available within the organisation, and how it is structured. Internal stakeholders and their expectations are part of the internal context.

Internal context is about the culture of the organisation, the resources that are available, receiving outputs from the risk management process and ensuring that these influence behaviours that support and provide governance of risk and risk management. The internal context concerns objectives, the capacity and capabilities of the organisation, as well as the business core processes that are in place. An important consideration regarding the internal context is how the organisation makes decisions.

Having discussed the context for the organisation, ISO 31000 provides considerable information on the risk management process and provides a diagram that is included in this guide as Figure 3. It should be noted that the risk management process is no longer represented as a series of linked activities with connecting arrows in the way that it was presented in the 2009 version of ISO 31000. The risk management process is now presented as a set of iterative steps that are undertaken in a coordinated manner, but not necessarily in a strict sequence.

In this regard, the new representation of the risk management process in ISO 31000 is similar to the approach taken by the 2004 COSO publication *Enterprise Risk Management — Integrated Framework* (COSO ERM cube). ISO 31000 acknowledges this similarity by stating: 'Although the risk management process is often presented as sequential, in practice it is iterative'.

At the centre of the risk management process are the activities of risk assessment and risk treatment. Risk assessment is described as having the three stages of risk identification, risk analysis and risk evaluation. Each of the three stages is described in detail in ISO 31000 and it provides valuable insight into how risks can be identified, how they can be analysed in terms of likelihood and consequences and finally, how they can be evaluated in relation to the established risk criteria (risk appetite) to determine whether additional action is required.

Risk treatment is also a vitally important part of the risk management process and ISO 31000 provides information on the selection of risk treatment options, the preparation and implementation of risk treatment plans. ISO 31000 states that the selection of risk treatment options involves balancing the potential benefits of introducing further risk treatment (controls) against the associated cost, effort or disadvantages. The risk treatment plan should clearly identify the timescale and responsibilities for implementing the selected risk treatments.

The guidelines provided in ISO 31000 includes information, advice and guidance on all the steps required to implement risk management and ensure continual improvement in performance. As illustrated in Section 8, there is a high degree of completeness in ISO 31000 compared with the requirements of Annex SL. Section 9 of this guide provides a consolidated approach to the implementation of a risk management initiative in terms of plan, implement, measure and the learn (PIML).

8. Comparison of ISO 31000 against Annex SL

ISO has published guidance on the format for management system standards as Annex SL and this format has been adopted for the most recent version of the quality standard ISO 9001:2015 *Quality management systems – Requirements*. Annex SL provides information on the components that are required in a full management system standard. Appendix A summarises the Annex SL format.

Figure 1 and Figure 2 in Section 2 of this guide illustrate the relationship between the seven substantive components of Annex SL. Figure 1 identifies the relationship between the 'Scope and Design' components of context, leadership and support. Figure 2 identifies the relationship between the 'Control and Develop' components of the plan, implement, measure and learn.

ISO 31000 provides separate narrative and guidance on the principles, framework and process for risk management. Separation presentation of principles, framework and process is not aligned with the format of Annex SL. This separation makes mapping of ISO 31000 against Annex SL challenging. Nevertheless, Table 3 provides a mapping of the framework and process components of ISO 31000 against Annex SL. The mapping demonstrates that ISO 31000 provides full coverage of the requirements for a management system standard.

Table 3: Mapping of ISO 31000 against Annex SL

Clause	Annex SL heading	ISO 31000 (2018)
1.	**Scope**	
2.	**Normative references**	
3.	**Terms and definitions**	
4.	**Context of the organisation**	
4.1	Understanding the organisation and its context	Component 2 of the Framework: 'Integration' includes determining oversight roles and responsibilities and ensuring RM is part of all aspects of the organisation Component 2 of the Process: 'Scope, context and criteria' includes purpose and scope of RM, defining risk criteria and risk decision-making
4.2	Understanding the needs and expectations of interested parties	
4.3	Determining the scope of the management system	
4.4	The management system	
5.	**Leadership**	
5.1	Leadership and commitment	Component 1 of the Framework: 'Leadership and commitment' includes aligning RM, policy statement, resources and risk appetite Component 3 of the Framework: 'Design' includes internal and external context, roles and responsibilities, and communications and consultation
5.2	Policy	
5.3	Organisational roles, responsibilities and authorities	
6.	**Planning**	
6.1	Actions to address risks and opportunities	Component 1 of the Framework: 'Leadership and commitment' includes aligning RM, policy statement, resources and risk appetite Component 3 of the Framework: 'Design' includes internal and external context, roles and responsibilities, and communications and consultation
6.2	Management system objectives and planning to achieve them	

7.	**Support**	
7.1	Resources	Component 1 of the Process: 'Communication and consultation' includes involvement, risk information and ownership of risk Component 6 of the Process: 'Recording and reporting' includes information for decision-making and risk information for stakeholders
7.2	Competence	
7.3	Awareness	
7.4	Communication	
7.5	Documented information	
8.	**Operation**	
8.1	Operational planning and control	Component 4 of the Framework: 'Implementation' includes implementation deadlines, decision-making and implementation responsibilities Component 3 of the Process: 'Risk assessment' includes description of the identification, analysis and evaluation stages of risk assessment Component 4 of the Process: 'Risk treatment' includes the selection, design and implementation of risk treatment options
9.	**Performance evaluation**	
9.1	Monitoring, measurement, analysis and evaluation	Component 5 of the Framework: 'Evaluation' includes measuring framework performance and continued suitability of the framework Component 5 of the Process: 'Monitoring and review' includes monitoring RM outcomes, and inclusion of risk within performance reports
9.2	Internal audit	
9.3	Management review	
10.	**Improvement**	
10.1	Non-conformity and corrective action	Component 6 of the Framework: 'Improvement' includes value of RM, adapting the framework and integration of RM activities
10.2	Continual improvement	

9. Relevance of ISO 31000 for risk professionals

The ISO 31000 guidance is presented in narrative form as a list of principles, framework and process. There are several examples in ISO 31000 of overlap between framework and process, as demonstrated by the inclusion of context as part of the designing the framework and as part of scope, context and criteria. Another example of the overlap of framework and process is that establishing communication and consultation is a component of the process and is discussed as part of the design component of the framework.

In addition to overlap of framework and process, there are examples of overlap of principles and framework, including the inclusion of integration as a principle and as a component of the framework. These overlaps demonstrate that risk professionals who use ISO 31000 as the basis for implementation of a risk management initiative will need to extract the valuable information and guidance provided in ISO 31000 and develop it into a coherent and logical implementation checklist.

Risk professionals need to understand the full and detailed requirements of a management system, as set out in Annex SL. These requirements define the components required for the successful implementation of a management initiative, including a risk management initiative. The list below provides an overview of the stages involved in implementing the 'Control and Develop' components of Annex SL.

Successful implementation of a risk management initiative is an ongoing process that involves working through the 10 activities below on a continuous basis. These activities relate to the four components (1) Plan; (2) Implement; (3) Measure; and (4) Learn.

Plan

1. Identify intended benefits of the RM initiative and gain board support
2. Plan the scope of the RM initiative and develop common language of risk
3. Establish the RM strategy, framework and the roles and responsibilities

Implement

4. Adopt suitable risk assessment tools and an agreed risk classification system
5. Establish risk benchmarks (risk criteria) and undertake risk assessments
6. Determine risk appetite and risk tolerance levels and evaluate the existing controls

Measure

7. Evaluate effectiveness of existing controls and introduce improvements
8. Embed risk-aware culture and align RM with other activities in the organisation

Learn

9. Monitor and review risk performance indicators to measure RM contribution
10. Report risk performance in line with obligations and monitor improvement

Although ISO 31000 covers the full scope of requirements for a management system, it is for the organisation to convert those requirements into a checklist and action plan. In fact, ISO 31000 covers the 'Control and Develop' components, as set out in Figure 2 in a concise and easy to understand manner. The 'Scope and Design' components from Annex SL are present in ISO 31000, but the structure of the guidelines on the framework require some interpretation and conversion into a checklist or implementation plan. The 2017 COSO framework *ERM – Integrating Strategy and Performance* provides an alternative approach that is also helpful.

There is much useful information in ISO 31000 for risk professionals as they support their employer and/or clients in the implementation of a risk management initiative. The combination of principles, framework and process set out in ISO 31000 provides a high-level, but comprehensive, view the components that are required to implement risk management in an organisation.

ISO 31000 is an important and well-recognised contribution towards effective risk management, but risk professionals will need to extract the guidance and advice most relevant to their employer or client organisations when formulating a successful risk management initiative that will enhance the success of the organisation.

Appendix A: Structure of ISO management system standards

ISO defines a management system as a set of procedures an organisation needs to follow in order to meet its objectives. A management system standard provides a model to follow when setting up and operating a management system. Some of the top-level benefits of a successful management system standard are (1) enhanced use of resources; (2) improved risk management; and (3) increased customer satisfaction by meeting product/service expectations.

ISO has published many management system standards for topics ranging from quality and environment to information security and business continuity management. Despite sharing common elements, ISO management system standards have sometimes had different structures. This has sometimes resulted in confusion and difficulties at the implementation stage.

Most organisations have more than one management system standard. Uncoordinated systems take up extra time and resources, so there is a clear need to find a way of integrating and combining the standards in the best possible way. Existing management system standards often have different structures, requirements and terminology, so integration is challenging. To address this problem, ISO developed Annex SL – the framework for a generic management system and the blueprint for all new and revised management system standards in future.

By adopting the Annex SL format, individual management systems will produce less duplication, confusion and misunderstandings. Management system auditors will be able to use a core set of generic requirements across disciplines and industry sectors. In future, all ISO management system standards will have the same high-level structure, identical core text, as well as common terms and definitions.

Annex SL applies to all management system standards, including full ISO standards. The revised ISO 9001 and ISO 14001, as well as the new ISO 45001 will all be based on the Annex SL high-level structure, as follows:

Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms and definitions
Clause 4: Context of the organisation
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement

Clause 1: Scope – sets out the intended outcomes of the management system. The outcomes are industry specific and should be aligned with the context of the organisation (see clause 4).

Clause 2: Normative references – provides details of the reference standards or publications relevant to the particular standard.

Clause 3: Terms & definitions – explains terms and definition applicable to the specific standard in addition to any formal related terms and definitions standard.

Clause 4: Context of the organisation – with four sub-clauses:

4.1 Understanding the organisation and its context
4.2 Understanding the needs and expectations of stakeholders
4.3 Determining the scope of the managements system
4.4 The management system

Clause 4 describes why the organisation exists. The organisation needs to identify internal and external issues that can impact on its intended outcomes, as well as all stakeholders and their expectations. It also needs to document its scope and set the boundaries of the management system.

Clause 5: Leadership – with three sub-clauses:

5.1 Leadership and commitment
5.2 Policy
5.3 Organisational roles, responsibilities and authorities

Top management is accountable for all management systems. They need to integrate the management system into core business process, ensure the system achieves its intended outcomes and allocate the necessary resources. Top management is also responsible for communicating the importance of the system to heighten employee awareness and involvement.

Clause 6: Planning – with two sub-clauses:

6.1 Actions to address risks and opportunities
6.2 Management system objectives and planning to achieve them

Having identified risks and opportunities, the organisation needs to specify how these risks will be managed. This

proactive approach replaces preventive actions and reduces the need for corrective actions later. The objectives of the management system should be measurable, monitored, communicated, aligned to the policy of the system and updated when needed.

Clause 7: Support – with five sub-clauses:

- **7.1** Resources
- **7.2** Competence
- **7.3** Awareness
- **7.4** Communication
- **7.5** Documented information

After addressing the context, commitment and planning, organisations need to look at the support needed to meet their goals and objectives. This includes resources, targeted internal and external communications, as well as documented information that replaces previously used terms such as documents, documentation and records.

Clause 8: Operation – with one sub-clause:

- **8.1** Operational planning and control

The bulk of the management system requirements specific to the topic under consideration are within this single clause. Clause 8 addresses both in-house and outsourced processes, while overall management of the process includes adequate criteria to control these processes, as well as ways to manage planned and unintended change.

Clause 9: Performance evaluation – with three sub-clauses:

- **9.1** Monitoring, measurement, analysis and evaluation
- **9.2** Internal audit
- **9.3** Management review

Decisions are required on how performance will be monitored, measured, analysed and evaluated. Internal audit activities are part of the process to ensure the management system conforms to the requirements of the organisation and is successfully implemented and maintained. Management review, evaluates whether the management system is suitable, adequate and effective.

Clause 10: Improvement – with two sub-clauses:

- **10.1** Non-conformity and corrective action
- **10.2** Continual improvement

Clause 10 looks at ways to address non-conformities and corrective action, as well as strategies for improvement on a continual basis. The requirement for continual improvement in performance and enhanced delivery of stakeholder expectations should be embedded in all management system standards.

https://www.bsigroup.com/LocalFiles/nl-nl/iso-9001/BSI-Annex-SL-Whitepaper.pdf

Appendix B: Components of ISO 31000:2018

1. Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives. Principles include the requirement for the risk management initiative to be (1) customised; (2) inclusive; (3) structured and comprehensive; (4) integrated; and (5) dynamic.

2. Framework

The purpose of the risk management framework is to assist with integrating risk management into all activities and functions. The effectiveness of risk management will depend on integration into governance and all other activities of the organisation, including decision-making.

1. Leadership and commitment, including:

- aligning risk management with the strategy, objectives and culture of the organisation;
- issuing a statement or policy that establishes a RM approach, plan or course of action;
- making necessary resources available for managing risk; and
- establishing the amount and type of risk that may or may not be taken (risk appetite).

2. Integration, including:

- determining management accountability and oversight roles and responsibilities; and
- ensuring risk management is part of, and not separate from, all aspects of the organisation.

3. Design, including:

- understanding the organisation and its internal and external context;
- articulating risk management commitment and allocating resources; and
- establishing communication and consultation arrangements.

4. Implementation, including:

- developing an appropriate implementation plan including deadlines;
- identifying where, when and how different types of decisions are made, and by whom; and
- modifying the applicable decision-making processes where necessary.

5. Evaluation, including:

- measuring framework performance against its purpose, implementation and behaviours; and
- determining whether it remains suitable to support achievement of objectives.

6. Improvement, including:

- continually monitoring and adapting the framework to address external and internal changes;
- taking actions to improve the value of risk management; and
- improving the suitability, adequacy and effectiveness of the RM framework.

3. Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

1. Communication and consultation, including:

- bringing different areas of expertise together for each step of the RM process;
- ensuring different views are considered when defining risk criteria and evaluating risks;
- providing sufficient information to facilitate risk oversight and decision-making; and
- building a sense of inclusiveness and ownership among those affected by risk.

2. Scope, context and criteria, including:

- defining the purpose and scope of risk management activities;
- identifying the external and internal context for the organisation;
- defining risk criteria by specifying the acceptable amount and type of risk; and
- defining criteria to evaluate the significance of risk and to support decision-making;

3. Risk assessment, including:

- risk identification to find, recognise and describe risks that might help or prevent achievement of objectives and the variety of tangible or intangible consequences;
- risk analysis of the nature and characteristics of risk, including the level of risk, risk sources, consequences,

likelihood, events, scenarios, controls and their effectiveness; and
- risk evaluation to support decisions by comparing the results of the risk analysis with the established risk criteria to determine the significance of risk.

4. Risk treatment, including:
- selecting the most appropriate risk treatment option(s); and
- designing risk treatment plans specifying how the treatment options will be implemented.

5. Monitoring and review, including:
- improving the quality and effectiveness of process design, implementation and outcomes;
- monitoring the RM process and its outcomes, with responsibilities clearly defined;
- planning, gathering and analysing information, recording results and providing feedback; and
- incorporating the results in performance management, measurement and reporting activities.

6. Recording and reporting, including:
- communicating risk management activities and outcomes across the organisation;
- providing information for decision-making;
- improving risk management activities; and
- providing risk information and interacting with stakeholders.

Institute of Risk Management
2nd Floor, Sackville House,
143-149Fenchurch Street,
London, EC3M 6BN
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org