From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks

Review of the 2004 and 2017 Enterprise Risk Management (ERM) frameworks published by COSO and commentary on the use of these frameworks by risk professionals

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on ERM, internal control and fraud deterrence.

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 enterprise risk management (ERM) and several different guides and risk management system standards have been published. This guide explains the approach used in the COSO ERM frameworks and identifies the importance and relevance of these frameworks. This guide also outlines the practical application of the COSO ERM frameworks and provides commentary on implementation.

It remains a challenge for risk professionals to clearly demonstrate the value of making resources available for ERM. In view of this continuing challenge, COSO has produced an updated version of the COSO ERM cube published in 2004 to bring greater focus to the positive contribution to performance that can be made by enterprise risk management.

The 2004 COSO Enterprise Risk Management — Integrated Framework (COSO ERM cube) and the more recent 2017 COSO ERM – Integrating Strategy and Performance publications are examples of risk management frameworks. An updated version of international risk management system standard ISO 31000 was published in early 2018 and an IRM guide to the updated ISO 31000 standard is published separately.

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

Annex SL provides seven substantive components of a management system standard and these are grouped in this guide as Scope and Design components and Control and Develop components. This guide considers these two elements of a management system standard and compares the COSO frameworks with the Annex SL format. The conclusion is that the COSO frameworks include all the required features of a management system standard, but with the emphasis on the Scope and Design components.

Overall, the COSO frameworks are strong on the context, leadership and support, but less detailed on the plan, implement, measure and learn features required of a management system standard. The message for risk professionals is that their employer or client organisations should implement the COSO components and principles that are best suited to their particular circumstances and modify other components and principles, as necessary.

The COSO ERM cube is still available from COSO and it is considered in this guide. In updating the ERM cube, COSO stated that organisations need to become more adaptive to change, and management needs to adopt better thinking on how to manage the increasing volatility, complexity and uncertainty in the marketplace. COSO has designed the updated framework to meet the needs of executive management and the board with a principles-based approach that integrates risk with strategy and performance.

2. Nature of management systems

A management system is the framework of policies, processes and procedures used by an organisation to ensure that it can fulfill all 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 their product quality and the consistency of products and/or services.

International Standards Organization (ISO) has published a guide to management system standards with details of the sections that should be included in a standard. 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 14001:2015 – *Environmental management systems* and ISO 45001 – *Occupational health and safety management systems*.

Given the well-established nature of Annex SL and the fact that the top selling ISO standard (ISO 9001) has already been converted into this format, it is the most appropriate structure against which to judge the risk management frameworks published by COSO. A summary of the Annex SL format is provided in Appendix A.

In order to undertake this comparison, and the subsequent evaluation of the COSO guidance, the Annex SL format components have been grouped into components that consider scope and design, followed by components that consider control and develop. The components relevant to the 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 described in this guide as plan, implement, measure and learn (PIML). This format is similar to the plan-do-check-act approach used by several management systems.

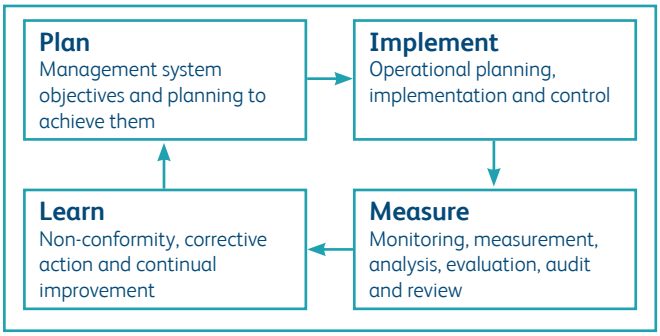
Figure 1 illustrates the relationship between the three components of the scope and design and Figure 2 demonstrates the relationship between the four components of control and develop. The presentation of the substantive seven components of Annex SL in this format is designed to separate the scope and design components, which represent the framework for supporting ERM from the control and develop components which represent the risk management process itself.

Formalised management systems have defined, documented processes that are designed 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 is why COSO has published ERM frameworks.

However, the COSO framework *Enterprise Risk Management – Integrating Strategy and Performance* and the international risk management system standard ISO 31000 are not in the Annex SL format for a management system standard. Therefore, the comparison in Table 1 in Section 7 of this guide is a useful means of testing the completeness of the COSO publications.

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 competitive landscape is defined by one word: disruption. The ideas of incremental progress, continuous improvement, and process optimizations do not work anymore. Those practices are necessary, but insufficient. It is now impossible to build enduring success without creating new ideas from within an organisation.

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 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, particularly at senior levels in the organisation and in the boardroom.

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 risks 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.

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

Traditionally, ERM has played a strong supporting role at board level. Now, boards are increasingly expected to provide robust oversight of ERM. ERM frameworks supply 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 organisational performance.

The need for organisations to have appropriate enterprise risk management activities in place has never been greater as the level of uncertainty facing organisations continues to grow. Organisations face a significant range of risks and many of these are related to the desire of many countries and/or regions to gain greater autonomy. This worldwide trend will increase trade protectionism and even increase the scope for regional conflicts.

4. Structure and approach of COSO guidance

COSO is a recognised body that has published guidance on risk management and internal control for some time. The publications most relevant to risk management are the 2004 *Enterprise Risk Management — Integrated Framework* (COSO ERM cube) and the more recent 2017 COSO ERM – *Integrating Strategy and Performance framework*. Also, COSO has published the highly influential *Internal Control — Integrated Framework* (2013) that is used as guidance to compliance with the Sarbanes Oxley Act of 2002.

Section 5 of this guide evaluates the COSO ERM cube and considers the components that are necessary to implement enterprise risk management. Section 6 of this guide considers the ERM – *Integrating Strategy and Performance* guidance from COSO and analyses the components and principles of enterprise risk management that are described.

In both cases, COSO presents the necessary actions as a series of components. In the COSO ERM cube, eight components are presented and in the 2017 framework, a total of five components are presented. These five components are then broken down into the supporting principles that are required if the component is to be delivered. A total of 20 principles are presented. A more detailed analysis of the principles and a brief description of each of the principles is set out in Appendix B.

Understanding the components is an important consideration when seeking to apply the COSO approach to the management of risk within an organisation. Section 7 of this guide compares the components in the COSO ERM cube and in the 2017 framework with the components of a management system, as described in Annex SL. Both the 2004 and 2017 ERM frameworks are currently available from COSO.

COSO published *Enterprise Risk Management — Integrated Framework* in 2004. The purpose of that publication was to help organisations better protect and enhance stakeholder value. In the 2017 framework, COSO starts with the premise that ERM enriches management dialogue by adding perspective to the strengths and weaknesses of a strategy, and whether a strategy fits with the mission and vision of the organisation. It allows management to feel more confident that they have examined alternative strategies and considered the consequences for the organisation when implementing the selected strategy.

Once strategy is set, ERM provides an effective way for management to fulfill its role, knowing that the organisation is attuned to risks that can impact strategy and is managing them well. All organisations need to set strategy and periodically adjust it, always staying aware of both ever-changing opportunities for creating value and the challenges embedded in pursuit of that value. To do that, they need the best possible framework for optimizing strategy and performance.

COSO has stated that organisations that integrate ERM throughout the organisation can realise many benefits, including, but not limited to:

- ***Increasing the range of opportunities:*** By considering all possibilities (both positive and negative aspects of risk), management can identify new opportunities and the challenges associated with current opportunities.
- ***Identifying and managing risk organisation-wide:*** Every organisation faces risks and a risk can originate in one part of the organisation but impact a different part. Management iden¬tifies and manages these organisation-wide risks to sustain and improve performance.
- ***Increasing positive outcomes and advantage while reducing negative surprises:*** ERM allows organisations to improve their ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses, while profiting from beneficial developments.
- ***Reducing performance variability:*** Performing beyond expectations may cause concern and ERM allows organisations to anticipate the risks that would affect

performance and put in place actions to minimise disruption and maximise opportunity.

- ***Improving resource deployment:*** Every risk could require resources. Obtaining robust information on risk allows management, in the face of finite resources, to assess overall resource needs, prioritise resource deploy¬ment and enhance resource allocation.
- ***Enhancing enterprise resilience:*** Longer-term viability depends on the ability to anticipate and respond to change. ERM facilitates resilience and this is increasingly important as the pace of change acceler¬ates and business complexity increases.

5. Guidance provided by the COSO ERM cube 2004

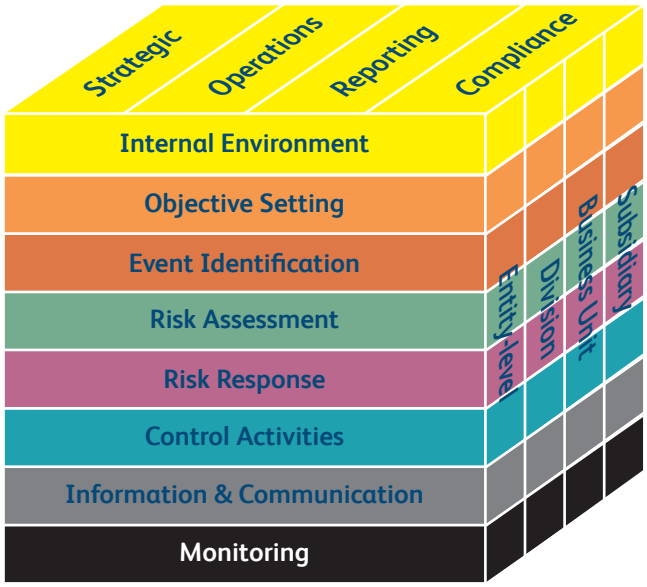
The COSO ERM cube remains important and influential because it provides a framework against which risk management and internal control systems can be assessed and improved. Corporate scandals, arising in companies where risk management and internal control were deficient, and the resulting attempts to further regulate corporate behaviour have resulted in increased interest in best practice in risk management.

The COSO ERM cube was published in 2004 and it is a well recognised ERM framework that is reproduced as Figure 3. In simple terms, in order to achieve a successful ERM initiative, an organisation needs to implement all eight components shown on the front of the cube in relation to each of the four risks indicated across the top in all parts of the organisation, as indicated on the side of the cube. This guide includes a description of the COSO ERM cube because it has not been withdrawn by COSO and it provides background to the publication of the 2017 framework.

The nature of the eight components and the actions required to implement the components are described in detail in the COSO guidance. The activities required to implement the eight components are briefly described below to facilitate comparison with Annex SL. It can be seen that the COSO ERM cube covers the components required by Annex SL. There is greater emphasis on the risk management process, covered by the Control and Develop components shown in Figure 2, as compared with the framework components, demonstrated by Scope and Design in Figure 1.

Figure 3: COSO ERM cube

Enterprise Risk Management – Integrated Framework



COSO use the cube to illustrate the links between business objectives on the top of the cube and the eight components shown on the front. These categories of business objectives are also the categories of risks that organisations face. The third dimension of the cube represents the business units of the organisation and illustrates that ERM should be implemented across all locations and all activities within the organisation.

1. Internal Environment

The internal environment establishes the tone of the organisation and influences attitudes towards risk management, risk appetite and ethical values. The guidance considers the impact of the competitive environment, regulation and external stakeholders on risk appetite and culture.

2. Objective Setting

The board should set objectives that support the mission of the organisation that are consistent with its risk appetite. If the board is to set objectives effectively, it needs to be aware of the risks arising if different objectives are pursued.

3. Event Identification

The organisation must identify internal and external events that affect the achievement of its objectives. The guidance draws a distinction between events having a negative impact that represent risks and events having a positive impact that represent opportunities.

4. Risk Assessment

The likelihood and impact of risks are assessed as a basis for determining how to manage them.

As well as mapping the likelihood and impact of individual risks, managers also need to consider how individual risks interrelate.

5. Risk Response

Management selects appropriate actions to align risks with risk appetite and tolerance. This stage can be seen in terms of the four main responses – reduce, accept, transfer or avoid. The guidance stresses the importance of taking a portfolio view of risk and not treating risks in isolation.

6. Control Activities

Policies and procedures should operate to ensure that risk responses are effective. Once designed, the controls in place need to operate properly. The ERM cube framework is supplemented by the guidance in Internal Control – Integrated Framework (2013).

7. Information and Communication

Information systems should ensure that data is identified, captured and communicated in a format and timeframe that enables managers and staff to carry out their responsibilities. The information provided to management needs to be relevant and of appropriate quality.

8. Monitoring

The management system should be monitored and modified if necessary. There is a distinction between regular review (ongoing monitoring) and periodic review (separate evaluation). The guidance stresses the importance of feedback and action.

The approach adopted by the COSO ERM cube suggests that ERM is not strictly a sequential set of activities, where one component affects only the next. It is a multidirectional, iterative process in which almost any component influences all other components. COSO sates that: within the context of the established mission or vision of an organisation, management establishes strategic objectives, selects strategy and sets aligned objectives cascading through the enterprise.

The next section of this guide considers the updated COSO ERM guidance. COSO has stated that since the adoption of the 2017 ERM – Integrating Strategy with Performance guidance is not mandatory, management may continue to utilise the COSO ERM cube. However, COSO reserves the right to supersede or retire the 2004 Enterprise Risk Management – Integrated Framework in the future.

6. Guidance provided by the COSO framework 2017

COSO decided to publish an updated version of their guidance on ERM in 2015 and published an exposure draft in 2016. This consultation led to the publication of revised guidance in 2017 entitled ERM – Integrating Strategy and Performance. COSO published this guidance in order to more clearly connect ERM with a multitude of stakeholder expectations; position risk in the context of performance, rather than as an isolated exercise; enable organisations to better anticipate risk, not simply the potential for crises; and provide an understanding that change creates opportunities.

The basis of the 2017 COSO guidance is that ERM should be embedded into the activities of an organisation, including the mission, vision and core values. In developing strategy, business and performance objectives, an organisation should consider the implications of the selected strategy; the risks to strategy and performance; and the possibility of the strategy not aligning with core values.

The possibility of strategy not aligning with mission, vision, and core values is central to strategy selection. Every organisation has a mission, vision and core values that define what it is trying to achieve and how it wants to conduct business. Mission, vision and core values matter most when it comes to managing risk and remaining resilient during periods of change. Also, there are implications for the strategy chosen, since each alternative strategy has its own risk profile. The board needs to determine if the strategy is compatible with risk appetite, and how it will influence objectives and efficient allocation of resources.

The 2017 COSO ERM framework clearly differentiates between ERM and internal control and enhances the references to risk appetite and risk tolerance. The intention of the framework is to elevate discussion of strategy, enhance the alignment between performance and more explicitly link ERM into decision-making. There is greater emphasis on the relationship between risk and value and also the benefits of integration of ERM. Finally, the framework underlines the role of culture in the achievement of successful ERM.

COSO suggests that over the longer term, ERM can also enhance enterprise resilience – the ability to anticipate and respond to change. It helps organisations identify factors that represent not just risk, but change, and how that change could impact performance and necessitate a shift in strategy. All organisations need to set strategy and periodically adjust it, always staying aware of both ever-changing opportunities for creating value and the challenges that occur in pursuit of that value.

Guidance is based on the five components shown in Figure 4, and each of these components is supported by three, four or five principles. It is by understanding the principles and implementing them fully that enhanced performance will be achieved from the ERM initiative. The components and associated principles are described in Appendix B and the components are summarised over the page.

Figure 4: Components of ERM

Enterprise Risk Management – Integrating Strategy with Performance © 2017. Committee of Sponsoring Organisations of the Treadway Commission (COSO). All rights reserved. Used with permission.

1. **Governance and Culture:** Governance sets the tone for the organisation and establishes oversight responsibilities for ERM. Culture relates to ethical values, desired behaviours and understanding of risk.
2. **Strategy and Objective-Setting:** ERM, strategy and objective-setting work together in the strategic-planning process. Risk appetite should be aligned with strategy and business objectives to successfully implement strategy.
3. **Performance:** Risks that can impact achievement of strategy and business objectives need to be identified and assessed and risks prioritised by severity in the context of risk appetite, so that risk responses can be selected.
4. **Review and Revision:** By reviewing organisation performance, an organisation can consider how well the ERM components are functioning over time and following substantial change, and what revisions are necessary.
5. **Information, Communication and Reporting:** ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organisation.

COSO has stated that organisations need to identify the best framework for optimizing strategy and performance in order to integrate ERM throughout the organisation to achieve benefits, including:

- identifying new opportunities;
- identify and manage risk organisation-wide to sustain and improve performance;
- increase positive outcomes and reduce negative surprises;
- reduce performance variability and minimise disruption;
- improve resource deployment and enhance resource allocation; and
- enhance enterprise resilience, not only to survive but also to evolve and thrive.

7. Comparison of COSO guidance 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 plan, implement, measure and learn.

Table 1 summarises the mapping of the COSO frameworks against Annex SL. Both the COSO ERM cube 2004, and the COSO framework 2017 provide full coverage of the Annex SL requirements for a management system standard. It is worth noting that the format used in the COSO publications is not the same as in Annex SL and the COSO frameworks are quite different in the way they present the information and the graphics that are used.

Table 1: Mapping of the COSO frameworks against Annex SL

Clause	Annex SL heading	COSO ERM cube (2004)	COSO framework 2017
4.	**Context of the organization**		
4.1	Understanding the organisation and its context	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 3: Event Identification includes internal and external events that could have positive or negative impact on objectives	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy & Objective-Setting includes context, risk appetite and setting of strategy and business objectives
4.2	Understanding the needs and expectations of stakeholders		
4.3	Determining the scope of the management system		
4.4	The management system		
5.	**Leadership**		
5.1	Leadership and commitment	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities
5.2	Policy		
5.3	Organisational roles, responsibilities and authorities		
6.	**Planning**		
6.1	Actions to address risks and opportunities	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy & Objective-Setting includes context, risk appetite and setting of strategy and business objectives
6.2	Management system objectives and planning to achieve them		

Clause	Annex SL heading	COSO ERM cube (2004)	COSO framework 2017
6.	**Planning**		
6.1	Actions to address risks and opportunities	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 2: Objective Setting includes mission and setting objectives consistent with risk appetite	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 2: Strategy & Objective-Setting includes context, risk appetite and setting of strategy and business objectives
6.2	Management system objectives and planning to achieve them		
7.	**Support**		
7.1	Resources	Component 1: Internal Environment includes risk appetite, attitude to RM, ethical values and stakeholder expectations Component 7: Information & Communication includes need for relevant quality information to be captured and communicated	Component 1: Governance & Culture includes board oversight, culture, ethical values, capabilities and responsibilities Component 5: Information, Communication & Reporting includes communication, use and reporting of risk information
7.2	Competence		
7.3	Awareness		
7.4	Communication		
7.5	Documented information		
8.	**Operation**		
8.1	Operational planning and control	Component 4: Risk Assessment includes determination of impact, likelihood and inter-relationships of risks Component 5: Risk Response includes actions to align portfolio of risks with risk tolerance and risk appetite	Component 3: Performance includes risk identification and assessment, risk response and inter-relationship of risks
9.	**Performance evaluation**		
9.1	Monitoring, measurement, analysis and evaluation	Component 6: Control Activities includes actions to ensure risk responses are effective and efficient Component 8: Monitoring includes need to monitor and modify the management system and review performance	Component 4: Review & Revision includes assessment of change, monitoring of risk performance and continual improvement
9.2	Internal audit		
9.3	Management review		
10.	**Improvement**		
10.1	Non-conformity and corrective action	Component 8: Monitoring includes need to monitor and modify the management system and review performance	Component 4: Review & Revision includes assessment of change, monitoring of risk performance and continual improvement
10.2	Continual improvement		

8. Relevance of COSO frameworks for risk professionals

Implementation of the COSO approach, both the COSO ERM cube and the COSO Integrating Strategy and Performance framework presents challenges. The guidance is presented in narrative form as a list of principles. Although both COSO frameworks cover the scope of requirements for a management system, it is for the organisation to convert those principles into an action plan. In fact, the COSO frameworks cover the Scope and Design components, as set out in Figure 1 in a concise and easy to understand manner. However, the Control and Develop components from Annex SL are not as clearly presented in the COSO publications, especially the Integrating Strategy and Performance framework 2017.

Risk professionals need to understand the requirements of a management system, as set out in Annex SL. These requirements define the components required for the successful implementation of an ERM initiative. In particular, the list below provides an overview of the stages involved in the implementation of the Control and Develop components of the initiative. Successful implementation of ERM activities is an ongoing process that involves working through the 10 steps below on a continuous basis. These 10 steps relate to the four components:

- **Plan**
- **Implement**
- **Measure**
- **Learn.**

Plan

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

Implement

4. Adopt suitable risk assessment tools and an agreed risk classification system
5. Establish risk benchmarks 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 ERM contribution
10. Report risk performance in line with obligations and monitor improvement

The 2017 framework on integrating strategy and performance provides a more detailed account of the Scope and Design components and the ERM cube provides a better approach to the Control and Develop components. Having identified the Context and Design components, it will then be possible to take a proposal to senior management identifying the resources required for the Control and Develop components in order to achieve successful implementation of the ERM initiative.

Many organisations focus on identifying risks to the execution of the strategy. However, COSO asserts that "risks to the strategy" is not the only dimension of risk to consider. There is the "possibility of strategy not aligning" with the mission, vision and core values. A misaligned strategy increases the possibility that, even if successfully executed, the organisation may not realise its mission and vision. This approach of challenging the selected strategy is one of the strengths of the 2017 COSO framework.

In summary, the "implications of the selected strategy" also need to be considered. COSO states that: "the board of directors and management need to consider how the strategy will impact risk appetite, and how it will help drive the organisation to set objectives and ultimately allocate resources efficiently."

Finally, risk professionals should consider the following features of the COSO frameworks that will need to be addressed as the COSO framework is implemented:

1. The COSO frameworks have more focus on the internal environment, rather than the influence of the business environment, regulatory conditions and external stakeholders.
2. Stakeholders expectations are not considered on the basis that many of the risks faced by organisations result from incompatibility between stakeholder and organisational objectives.
3. COSO ERM risks are mostly about losses and risk response is about reducing the likelihood and severity of losses, rather than examining the taking of risk to achieve return.
4. The COSO documents do not differentiate between the Scope and Design components with the Control and Develop components, as described in Figures 1 and 2.

Appendix A: Structure 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 using the Annex SL format, management systems will produce less duplication, confusion and the 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 (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 definitions applicable to the specific standard in addition to any formal related terms and standard definitions.

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 the whole management system. They need to integrate the management system into core business process, ensure the system achieves its intended outcomes and allocates 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 preventative action 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: Operations – 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 the overall process management 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 in place.

10.1 Non-conformity and corrective action
10.2 Continual improvement

Clause 10 looks at ways to address non-conformities and take 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 the COSO framework 2017

Figure B1 lists the five components and 20 principles described in the COSO framework *Enterprise Risk Management – Integrating Strategy with Performance*. This appendix provides summary information on each of the components and principles. COSO states that implementation of all 20 principles is required in order to achieve successful integration of enterprise risk management with strategy and performance.

Figure B1: Components and Principles of ERM

1. Governance & Culture

Risk governance sets the tone and reinforces the importance of ERM oversight. Culture is reflected in decision-making and includes ethical values and responsible business behaviour. Both governance and culture are needed for effective ERM. There are five principles for this component.

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops and Retains Capable Individuals

1. Exercises Board Risk Oversight – Risk governance and culture start at the top with the influence and oversight of the board. Board members must be accountable and responsible for risk oversight and possess the required skills, experience and business knowledge.

2. Establishes Operating Structures – Strategy is executed by organisation and execution of day-to-day operations to achieve business objectives. How the operating model is administered and governed can introduce new and different risks or complexities.

3. Defines Desired Culture – COSO frames desired behaviours within the context of culture, core values and attitudes toward risk. Whether an organisation considers itself to be risk averse, risk neutral or risk aggressive, it should have a risk-aware culture.

4. Demonstrates Commitment to Core Values – Culture and tone at the top is defined by the operating style and personal conduct of management and the board of directors and it must be driven deep down into the organisation.

5. Attracts, Develops and Retains Capable Individuals – Management must define the knowledge, skills and experience needed to execute strategy; set appropriate performance targets; attract, develop and retain appropriate personnel and strategic partners; and arrange for succession.

2. Strategy & Objective-Setting

The updated COSO framework elevates the discussion of strategy and the integration of ERM with strategy by asserting that all aspects and implications of strategy need to be considered when setting strategy. There are four principles for this component.

6. Analyses Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

6. Analyses Business Context – The updated framework considers business context and the role of internal and external stakeholders. The point is that management must consider risk from changes in business context and adapt accordingly in executing strategy.

7. Defines Risk Appetite – The organisation defines risk appetite in the context of creating, preserving and realising value. The risk appetite statement is considered during strategy setting, communicated by management, embraced by the board and integrated across the organisation.

8. Evaluates Alternative Strategies – Alternative strategies are built on different assumptions – and those assumptions may be sensitive to change. The organisation evaluates strategic options and sets its strategy to enhance value, considering risk resulting from the strategy chosen.

9. Formulates Business Objectives – Management establishes objectives that align with and support the strategy at various levels of the business. These objectives should consider, and be aligned with, risk appetite.

3. Performance

Risks that could impact achievement of strategy and objectives should be identified and assessed. These risks must be prioritised in terms of severity in the context of risk appetite. Risk responses should be selected to form a portfolio view of risk. There are five principles for this component.

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritises Risk
13. Implements Risk Responses
14. Develops a Portfolio View

10. Identifies Risk – The organisation identifies new and emerging risks, as well as changes to known risks to the execution of its strategy. The risk identification process should consider risks arising from a change in business context and risks currently existing but not yet known.

11. Assesses Severity of Risk – Depending on the anticipated severity of the risk, COSO suggests the use of qualitative and quantitative approaches in assessment processes. Scenario analysis may be appropriate in assessing risks that could have an extreme impact.

12. Prioritises Risk – The organisation prioritises risks as a basis for selecting risk responses using appropriate criteria. Risk criteria might include adaptability, complexity, velocity, persistence and recovery, as well as acceptable variation in performance.

13. Implements Risk Responses – Risk responses may accept, avoid, exploit, reduce and share risk. In selecting risk responses, management considers such factors as the business context, costs and benefits, severity of the risk, and the appetite for risk.

14. Develops Portfolio View – Portfolio view is a composite view of the risks the organisation faces relative to business objectives, which allows management and the board to consider the nature, likelihood, relative size and interdependencies of risks, and how they may affect performance.

4. Review & Revision

The fourth component focuses on monitoring risk management performance. Effective monitoring provides insight into the relationship between risk and performance, how strategic risks are affecting performance, and emerging risks. There are three principles for this component.

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in ERM

15. Assesses Substantial Change – Change can create significant competitor performance gaps or invalidate critical assumptions underlying strategy. Monitoring substantial change is built into business processes in the ordinary course of running the business.

16. Reviews Risk and Performance – Risk responses must be evaluated to ensure they are performing as intended. The task of assessing risk responses is typically owned by those accountable for the effective management of identified risks and by assurance providers.

17. Pursues Improvement in ERM – ERM should be improved continuously over time. Even mature ERM processes can become more efficient and effective in increasing its value contributed. Embedding continuous evaluations can systematically identify improvements.

5. Information, Communication & Reporting

The final component recognises the vital need for a continuous process to obtain and share relevant information. This information for decision-making must flow up, down and across the organisation and provide insight to key stakeholders. There are three principles for this component.

18. Leverages Information Systems
19. Communicates Risk Information
20. Reports on Risk, Culture and Performance

18. Leverages Information and Technology – Information systems provide the organisation with the data and information to support ERM. Factors influencing technology selection include the strategy, marketplace needs, competitive requirements, and the associated costs and benefits.

19. Communicates Risk Information – The organisation reports on risk at multiple levels across the organisation. Organisations use different channels to communicate risk data and information to internal and external stakeholders.

20. Reports on Risk, Culture and Performance – Risk reporting encompasses information required to support decision-making and enable the board and others to fulfill their risk oversight responsibilities. There are many different types of reports on risk, culture and performance.

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