ISSN 2389-8186
E-ISSN 2389-8194

Vol. 4, No. 2
Septiembre de 2017
doi: http://dx.doi.org/10.16967/rpe.v4n2a7

ARTÍCULOS ORIGINALES

# A more effective audit after COSO ERM 2017 or after ISO 31000:2009?

**ALCINA PORTUGAL DIAS**[a]

pp. 73-82

**ABSTRACT** This paper seeks to consider the better effectiveness of an audit after the use of ERM 2017 or ISO 31000. To this effect, is COSO existence and evolution will be considered and related to the biggest financial scandals and its output in terms of control schedules. Some criticisms to COSO Cube will be pointed out, and the new ERM 2017 will be described. ISO 31000 will be considered as an alternative guideline to be used for Risk Management purposes in any organization. A comparison is made between the two sets of Risk management. The audit process will be developed after grasping that the company has a risk management implemented in a more certain fashion, as objectives are different but schemes of risk management control are valid. In terms of future research perspective, one could suggest the identification of organizations using one scheme (ERM) or another (ISO), analysing them and comparing them in order to evaluate their particular effectiveness and accrued value.

**KEYWORDS** Financial frauds, COSO, ISO 31000, ERM 2017, audit.

**HISTORIA DEL ARTÍCULO**

**¿CÓMO CITAR?:**
Dias, A. P. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000:2009?. *Perspectiva Empresarial*, *4*(2), 73-82. http://dx.doi.org/10.16967/rpe.v4n2a7

**RECIBIDO:** 18 de junio de 2017
**APROBADO:** 17 de agosto de 2017

**CORRESPONDENCIA:**
Alcina Portugal Dias, Jaime Lopes Amorim 465-004 Matosinhos tel 229050000, Portugal.

[a] *PhD, Professor at CEOS.PP – Centre for Organisational and Social Studies of P. Porto; APQ- SCOPE; UNIAG; EUROPAGUNE (Universidade do Pais Vasco). Instituto Superior de Contabilidade e Administração do Porto. E-mail: alcina @iscap.ipp.pt*

ISSN 2389-8186
E-ISSN 2389-8194

Vol. 4, No. 2
Septiembre de 2017
doi: http://dx.doi.org/10.16967/rpe.v4n2a7

# ¿Una auditoría más eficaz después del COSO ERM 2017 o de la ISO 31000:2009?

**RESUMEN** En este artículo se busca examinar la mayor efectividad de una auditoría después del uso del marco ERM 2017 o de la norma ISO 31000. A tal efecto, se considerará la existencia y evolución del COSO y se relacionará con los mayores escándalos financieros y sus resultados en términos de cronogramas de control. Se señalarán algunas críticas a COSO Cube y se describirá el nuevo marco ERM 2017. Por otra parte, la norma ISO 31000 se considerará como una directriz alternativa que se utilizará para fines de gestión de riesgos en cualquier organización. Se realiza una comparación entre las dos formas de gestión de riesgos. El proceso de auditoría se desarrollará después de comprender que la empresa cuenta con un proceso de gestión de riesgos implementado de cierta manera, puesto que los objetivos son diferentes pero los esquemas de control de gestión de riesgos son válidos. En términos de perspectiva para futuras investigaciones, se podría sugerir la identificación de organizaciones que utilizan un esquema (ERM) u otro (ISO), en el que se analicen y se comparen para evaluar su efectividad particular y valor acumulado.

**PALABRAS CLAVE** fraudes financieros, COSO, ISO 31000, ERM 2017, auditoría.

**¿CÓMO CITO EL ARTÍCULO?**
*HOW TO CITE THIS PAPER?*

**CHICAGO:**
Dias, Alcina Portugal. 2017. A more effective audit after COSO ERM 2017 or after ISO 31000:2009?". *Perspectiva Empresarial* 4(2): 73-82. http://dx.doi.org/10.16967/rpe.v4n2a7

**MLA:**
Dias, Alcina Portugal. "A more effective audit after COSO ERM 2017 or after ISO 31000:2009?". *Perspectiva Empresarial* 4.2 (2017): 73-82. Digital. http://dx.doi.org/10.16967/rpe.v4n2a7

## Uma auditoria mais efetiva depois do COSO ERM 2017 ou do ISO 31000:2009?

**RESUMO** Este artigo busca considerar a maior efetividade de uma auditoria depois do uso de ERM 2017 ou ISO 31000. Para isso, a existência e evolução do COSO será considerada e relacionada aos maiores escândalos financeiros e a sua saída em termos de programas de controle. Algumas críticas ao COSO Cube serão levantadas e o novo ERM 2017 será descrito. A ISO 31000 será considerada uma diretriz alternativa a ser usada pelos propósitos do Gerenciamento de Risco em qualquer organização. Uma comparação PE feita entre dois tipos de Gerenciamento de Risco. O processo auditado será desenvolvido depois de entender que a companhia tem gerenciamento de risco implementado de uma forma específica, assim como os objetivos são diferentes, mas os esquemas de controle de gerenciamento de risco são válidos. Em termos de perspectiva de futuras pesquisas, poderíamos sugerir a identificação de organizações usando um esquema (ERM) ou outro (ISO), analisando-os e comparando-os de forma a avaliar sua efetividade particular e valor acumulado.

**PALAVRAS CHAVE** auditoria, COSO, ERM 2017, fraudes financeiras, ISO 31000.

## Introduction

This paper seeks to look at COSO principles as something crucial for the achievement of any audit, particularly as concerns Enterprise Risk Management (ERM). At the same time, we aim to reflect about the use of ISO 31000 as an alternative guideline for risk management. The financial scandals will be named as a mobile for the development and implementation of control procedures and measures attributed to the internal control. Therefore, ERM 2017 will be described and ISO 31000 will be named as an alternative to it. A final consideration will be given in regards to the effects of these different risk control issues ERM/ ISO and their effect on audit procedures.

### 1. Financial scandals

Enron, Parmalat and Worldcom – among many others – were financial frauds that shocked the finance world, and deceived the stakeholders promising high dividends for something that was worth nothing at all (Merton, Peron,1993; Anomaly *et al* 2014; Donaldson, Preston 1995). Companies tried to increase profits by dissimulating debt using fraudulent devices, false increase of assets value, and schemes that constructed accrued income thus facilitating good profits and high dividend distribution. High dividends make shareholders happy and greedy for more and more. Companies do feel happy too because people want to join them and buy their equity. Thus, money comes in and shareholders are glad because they get more and more money. Nevertheless, they do not pay attention to the accuracy of the disclosure of the financial statements. They just believe in it and all the people involved in their process, until someone shows some evidence about reality revealing that the financial statements disclosed by the company are not true at all. This way, stakeholders are defrauded (Donaldson, Preston 1995). Their expectation is is actually quite different from reality. These events were violating the main ideas of the theories in table 1.

As for Accounting theory, all the principles associated to the preparation of financial statements were breached and overpassed (Business Press Ed, 2004; Wolk *et al, 2008).* This way if the disclosure of the financial statements is not trustful the CSR theory (Dion, 2001; Frynas, Stephan, 2015) is also being breached; all the stakeholders (Donaldson & Preston, 1995) have been deceived, and this has in impact in all parties related to companies - the society, the shareholders, the employees, the government and others. As companies fail and file for bankruptcy, all the principles and ideas that literature mentions about economic and political principles (Anomaly *et a*l, 2014) are put aside. All the concepts and ideas to be considered in order to rule an organization effectively are violated, and this has serious consequences on the business (Merton & Peron 1995) as a whole. In the end, one could also question the principles of legitimacy (Suchman, 1995) when considering that the right things on the right place were not working at all. This means that the values, tradition and culture of the organization were put aside and the inherent hierarchy was violated. Consequently, this leads us to the institutional perspective (Bruton, Ahlstrom, Li, 2010). As to the ethical issues (Bruton, Ahlstrom, Li, 2010), and these remain the most relevant effects of these financial scandals.

These financial scandals contributed to a shake on the financial American market. One can quote on a PESTES analysis perspective: Political, Economic, Social, Technological, Environmental and Sustainable. The big consequence of these events led to the need felt by SEC - Securities Exchange Commission and all the representative associations of accounting, auditing and management among others of organizing a committee that should rule the enterprise supervision.

**TABLE 1.** Financial scandals and the violation of the principles

| THEORIES | LITERATURE SOURCE |
|---|---|
| ACCOUNTING | Business Press Ed, 2004; Wolk et al, 2008 |
| CORPORATE SOCIAL RESPONSIBILITY (CSR) | Dion, 2001; Frynas, Stephan, 2015 |
| POLITICAL ECONOMY | Anomaly, Jonny & Brennan, Geoffrey,2014 |
| LEGITIMACY | Suchman, 1995 |
| STAKEHOLDER | Donaldson & Preston, 1995 |
| INSTITUTIONAL | Bruton, Ahlstrom, Li, 2010 |
| ETHICS | Dion, 2001; Frynas & Stephan, 2015 |
| BUSINESS | Merton & Peron 1995 |

## 2. COSO - Committee of Sponsoring Organizations of the Treadway Commission

These financial scandals – which basically took place starting in 2001 in the USA – caused serious reactions on the supervising financial entities. COSO – Committee of Sponsoring Organizations of the Treadway Commission, impelled by SEC - Securities Exchange Commission, issued procedures and guidelines for the reinforcement of the organization's internal control and risk management. Let us look at COSO evolution from its creation (table 2).

First of all, it is important to clarify the name of this Committee (devoted to make companies responsible for the preparation, reporting and disclosure of their financial statements). COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission). The first chairman of the National Commission was *James* C. Treadway, Jr., Executive Vice President and General Counsel. Paine Webber Incorporated and was a *former Commissioner* of the U.S. Securities and Exchange Commission. Treadway Commission was originally jointly sponsored and founded by five main professional accounting associations and institutes headquartered in the United States:

| | |
|---|---|
| American Institute of Certified Public Accountants | AICPA |
| American Accounting Association | AAA |
| Financial Executives International | FEI |
| Institute of Internal Auditors | IIA |
| Institute of Management Accountants | IMA |

The Treadway Commission recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control. These five organizations formed what is currently known as the Committee of Sponsoring Organizations of the Treadway Commission. COSO developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions. It included representatives from the industry, public accounting, investment firms, and the New York Stock Exchange. In 2002, the *control framework* was issued by COSO at the same time that Sox act was in force. Again, *Financial Reporting* was considered in 2006 by COSO. In parallel to all these measures of reinforcement of the internal control, the worldwide dissemination and implementation of IFRS (International Financial Reporting Standards) and ISA (International Standards on Audit) became something crucial for the global harmonization of accounting and reporting.

In 2016, COSO reviewed the final paper about ERM entitled *Aligning Risk with Strategy and Performance.* The output came out in 2017. The following objectives as to strategy and the role of ERM were redefined:

**TABLE 3.** New objectives of COSO ERM 2017

| OBJECTIVES |
|---|
| Enhance alignment between performance and ERM |
| Accommodate expectation for governance and oversight |
| Recognize globalization and need to apply a common albeit tailored approach |
| Present new ways to view risk in setting and achieving objectives in the context of greater complexity |
| Expand reporting to address greater transparency |
| Accommodate evolving technology |

**TABLE 2.** COSO evolution till 2006

| | 1934 | 1985 | 1992 | 2001/02 | SOx 02 | 2003 | 2006 |
|---|---|---|---|---|---|---|---|
| **USA** | **SEC** | **COSO (start)** | **COSO Control Framework** | **Biggest financial scandals** | **Sarbannes Paul, Oxley Michael** (*USA Senators*) **= SOX ACT IFRS and ISA's** | IFAC Credibility Report IFRS and ISA's | COSO Financial Reporting IFRS and ISA's |
| **EU and WORLD** | | ↓ | | **Biggest financial scandals** | **Canadian Bill 198, Loi sur la Secutité Française, Turnbull Guidance UK, J-SOX (2007) Japan IFRS and ISA's** | European Directives about Internal control IFRS and ISA's | European Directives IFRS and ISA's |

**FIGURE 1.** ERM 2017


Source: https://commsrisk.com/new-coso-erm-framework-out-for-comment

In sum, one can say that this update retitles the framework as Enterprise Risk Management—Aligning Risk with Strategy and Performance. This update also recognizes the importance of strategy and entity performance, and delineates between internal control and enterprise risk management by integrating enterprise risk management with decision making. One may think that COSO - ERM could answer some questions, suggestions and criticisms from the literature. The new figure for COSO will not be anymore the famous Cube but this new one (Figure 1).

The transformation of the COSO ERM cube in a COSO ERM process makes a new approach of risk management: it is a way of transforming inputs into outputs. It means that the perspective of ERM for any kind of organization has an input of deep knowledge of the mission, vision and core values of the organization, which becomes crucial for grasping the risks associated. This belief usually arrives from the top management, combined with the good management of – human and material – resources of the organization will enhance good performance. To reach this increased performance, we must take care and look at the organization under a risk framework perspective: risk governance and culture associated to the top of the hierarchy; risk strategy linked to objective setting connected to the strategic business units; risk in execution – meaning that risk found in the areas or sectors is being treated – risk information communication and reporting should inform all the parties involved in the organization about the state of art of the specific and related risk environment. Lastly, this risk analysis process makes a final evaluation of its existence – it must monitor the enterprise risk management performance. Perhaps this will be a challenging part to achieve. To perform effectively ERM, a large and deep risk analysis must be conducted because the points and reasons for events presenting a risk are so many and so different, that when evaluation is conducted on one risk, another may emerge that was not previously estimated. Yet this new COSO ERM seems to be quite different from the previous one. One may say that this COSO update is eventually a reaction to all the criticisms and suggestions made along the years. Literature – as explained below – revealed some opinions that were quite far away from the traditional inspiration of COSO described in a closed risk management cube.

## 3. Some criticism about COSO

Demidenko and MacNutt (2010) state that an ethical maturity scale based on duty and responsibility for practical implementation to ensure better governance should be considered, besides contributing with theoretical tenets to the debate on good governance and ethics of enterprise risk management (ERM).

Williamson (2007) says that COSO's (2004) framework on Enterprise Risk Management (ERM) makes a valuable contribution to the emerging practice of ERM, but has serious limitations. It fails to provide a workable standard for identifying ERM effectiveness. Its definition of 'risk' diverts attention from opportunities and from uncertainties that fall outside its closed rational systems perspective. By taking a command and control approach, it ignores shared management of uncertainties with external parties and social implications of ERM. As a result, threats will be created if this framework is widely followed, which seems likely as ERM is institutionalized within regulations, professional practice and expected norms of good management. Besides, a Canadian survey from 2007 considering the COSO approach revealed that the major technical weaknesses of COSO ERM were as follows: (table 4).

These criticisms seem to have been considered in this new COSO ERM 2017. Instead of a cube, we get a process with a *way in* and a *way out* considering the culture event - a most important issue that was not mentioned in the previous scheme. Besides this new approach of COSO, we should mention that many companies have used an alternative solution – ISO 31000.

## 4. ISO 31000

Many companies prefer to use this standard on Risk Management (ISO 31000) because it is easier to work with. This standard content is briefly summarized below in Figure 2, and detailed information is described in annex 1.

- **Establish the context**: first of all, the company has to define the context for the risk analysis, and it means the limits of the organization activity development that can be affected by risk. This way, we are defining the scope of application of the risk analysis. Some features of the company will be considered for this purpose: the environment, the values, the hierarchy, the leadership and the aim of the organization. This almost fits in the input of New COSO ERM.

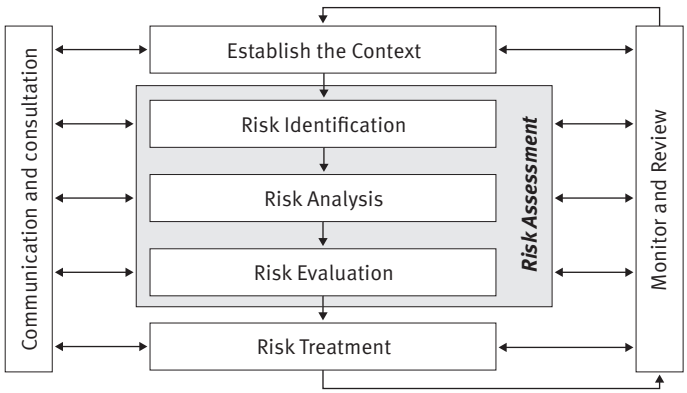
- **Risk assessment**: risk must be evaluated under the abovementioned context - it must be identified, analyzed and evaluated. Context risk is evaluated following the structure of the organization. Subsequently, its origin will be analyzed and the occurring effects will be evaluated. Only when these phases are surpassed can one have an idea of how much that risk matters –its importance or relevance.

**TABLE 4.** Some weaknesses of COSO

| TECHNICAL WEAKNESSES OF **COSO ERM** | |
|---|---|
| It is internally focused and the context is not established in terms of both external and internal factors and influences | "Risk responses", "control activities" and "monitoring" are confused. Control is used as both a verb and a noun |
| Stakeholders and their objective are ignored in terms of setting risk criteria | Risks are said to "occur" and likelihood is when risks occur |
| Risks are seen as events, not associated with the effect of uncertainty on objectives | Inherent risk is used: this is seen as a highly confusing and flawed concept that is unnecessary. |
| Risk is incorrectly estimated in terms of the likelihood of an event and its consequences. This produces 'phantom risks' and does not lead to effective and appropriate risk treatment | "Risk appetite" and "risk tolerance" are mixed up and confused. They are dealt with in a naive and simplistic way |
| Risks are only seen in a negative light and risk treatment (response) is only about mitigation | The description of the risk management process is mixed up with the framework required for the effective implementation of risk management through integration |

Source: Canadian Survey 2007

**FIGURE 2.** ISO 31000:2009




Source: http://broadleaf.com.au/resource-material/iso-31000-2009-setting-a-new-standard-for-risk-management

- **Risk treatment**: this is the last phase of the process. It means all the procedures needed in order to prevent risk from materializing.

After ISO 31000 implementation in an organization, all these steps – context, risk assessment and risk treatment – must be continuously monitored and reviewed through the achievement of audit. The final conclusions are addressed and communicated to all the people involved in the process at the organization. It seems to be a simple and easy way to face and position the organization's risks. A comparison between the New Process of COSO - ERM and ISO 31000 can be done (see table 5).

The numbers used in the abovementioned table as to ISO 31000 will be used to identify the equivalent subjects about ERM 2017 in table 6.

Below is an explanation of Table 5 (numbers 1 through 5), also known as ISO 31000:

1. Establish the context Risk and governance/ culture: context risk means the scope of application of the risk analysis. To do this, some features of the company will be considered: environment, values, hierarchy, leadership and the aim of the organization will be

**TABLE 5.** ISO 31000 brief summary

| ISO 31000:2009 | | |
|---|---|---|
| Consultation and communication | Establish the context | Monitor and review |
| | Risk assessment | |
| | identification | |
| | analysis | |
| | evaluation | |
| | Risk treatment | |

**TABLE 6.** COSO - ERM 2017

| ERM 2017 – NEW PROCESS | CONNECTION TO THE ORGANIZATION STRUCTURE |
|---|---|
| Risk governance /culture (1) | Top management |
| Risk strategy /objective setting (1) and (2.1) | SBU- Strategic Business Units |
| Risk in execution (2.2) and (2.3) | Functional level |
| Risk information, communication, reporting (4) | MIS – Management Information Systems and risk analysis |
| Monitoring ERM performance (5) | All the processes *in and across* the organization |

considered. Under ISO, risk strategy and the objectives are included in this context whilst they are autonomous for ERM 2017. This almost fits the input of New COSO regarding risk governance and culture. Risk governance is a kind of umbrella over the risk of the company, and culture means the perception of the values which are important for the company's development activity. This is usually obtained from contact with the top management of the company.

2. Risk assessment is an item that belongs just to ISO, and it means risk evaluation as a result of:
   - ***Risk identification*** which for ERM 2017 is associated to the objective setting; – ***Analysis of the risk*** dealing with the causes of the risk what for ERM 2017 is referred as risk in execution; – ***Risk evaluation*** something that is only considered, at this stage of analysis, by ISO 31000 meaning that after identifying and analyzing the risk we are able to evaluate it. For ERM 2017, this is done at the end, measuring the performance of the company after implementing the risk management (5).
3. Risk treatment for ISO means that something was really done. All the procedures needed were undertaken in order to prevent risk from happening. For COSO, this may be found in the last phase - monitoring ERM performance (5).
4. Whereas "Consultation and communication" is present in each part of the process under ISO, for ERM 2017 it appears at the end of the process (4).
5. Monitoring and reviewing are included both in ISO and ERM 2017. Under ISO, it is an interactive process applicable in each moment of each stage of the process, and ERM focuses on risk management and intends to evaluate its performance in the company.

## Conclusion

It is well known that good control of the internal procedures of any kind of organization will help the audit process, enabling some assurance about the opinion concerning the respective financial statements.

According to the literature (Williamson, 2007; Demidenko and MacNutt, 2010), COSO was regarded as a challenging perspective. ERM 2017 was described and ISO 31000:2009 (Risk Management) was considered as an alternative to it. The two sets of guidelines were considered and compared on a basis of risk management. The contents of both (ISO versus ERM) were analyzed, and it must argued that they are quite focused on the same issues. However, it seems that ISO was quite innovative a long time before the ERM update in 2017.

Implementation will depend on the organization profile and likeliness for a different use of risk guidelines. Companies that used to work with ISO – mainly the ones that have the ISO 9001 quality certification – would probably deal better with ISO 31000. Yet one must say that this new version of ERM seems to be a version which is quite well adapted to the global market, as well as to its organizations.

### Future research developments

In terms of future research, one could suggest the identification of organizations using one scheme (ERM) or the other (ISO) and compare them and try to evaluate their particular effectiveness and accrued value.

## REFERENCES

Accounting Theory, (2004) 4th Edition, U.K, Business Press Thomson Learning

Anomaly, Jonny & Brennan, Geoffrey (2014). Social Norms, The Invisible Hand, and the Law. *University of Queensland Law Journal* 33 (2).

Bruton, Ahlstrom, Li (2010) Institutional Theory and Entrepreneurship: Where Are We Now and Where Do We Need to Move in the Future? *Entrepreneurship Theory and Practice,*3 (3) pp 421–440

Dermot Williamson (2007). The COSO ERM framework: a critique from systems theory of management control, *International Journal of Risk Assessment and Management*, 7(8), pp 1089-1119, **doi**: http://dx.doi.org/10.1504/IJRAM.2007.015296

Dion, M.( 2001), 'Corporate Citizenship and Ethics of Care: Corporate Values, Codes of Ethics and Global Governance', in J. Andriof and M. McIntosh (ed.), *Perspectives on Corporate Citizenship* (Greenleaf, Sheffield, UK), pp. 118–138

Donaldson, Preston (1995) The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications *Academy of Management Review,* vol. 20, 1, pp 65-91

Elena Demidenko, Patrick McNutt (2010). "The ethics of enterprise risk management as a key component of corporate governance", *International Journal of Social Economics*, 37 (10), pp.802-815, doi: 10.1108/03068291011070462

Frynas G., Stephan S., (2015) Political Corporate Social Responsibility: Reviewing Theories and Setting New Agendas, *International Journal of Review Management*, 17(4), pp. 483–509

IIA Institute of Internal Auditors - Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls (2012)

Mark C. Suchman (1995) Managing Legitimacy: Strategic and Institutional Approaches ,*Academy Management Review , 20(3) 571-610;*

Merton, R., Peron, A.,(1993) Theory of risk capital in financial firms, *Applied Corporate Finance,* 6 (3), pp 16–32

OECD (2014), *Risk Management and Corporate Governance*, Corporate Governance, OECD Publishing. http://dx.doi.org/10.1787/9789264208636-en

Omolehinwa, O. (2003), Foundation of Accounting, Lagos Pumark Nigeria Ltd.

Ponemon Institute LLC (2013), *The State of Risk-Based Security*.

Schroeder, H. (2014), "An art and science approach to strategic risk management", *Strategic Direction*, Vol. 30 No 4 2014, pp. 28-30.

Wolk Harry I, Dodd James L and Rozycki John J (2008). Accounting Theory: Conceptual Issues in a Political and Economic Environment, 7th edition, Sage Publications Inc. California

World Business Council for Sustainable Development (WBCSD) http://www.wbcsd.org/.

World Economic Forum (2016), *The Global Risks Report 2016*, 11th edition.

## On line references

Canada Survey (2007): n*a.theiia.org/standardsguidance/Public%20Documents/IIA_Risk_Summit_Practitioner_Answers.pdf*

ISO 31000:2009 *http://broadleaf.com.au/resource-material/iso-31000-2009-setting-a-new-standard-for-risk-management*

COSO ERM 2017 https://commsrisk.com/new-coso-erm-framework-out-for-comment

**Annex 1. Relationships between risk management principles, framework and process**