Open University of Cyprus

Faculty

ECONOMICS AND

MANAGEMENT

Postgraduate Programme of Study *ENTERPRISE RISK MANAGEMENT*

Master's Dissertation

ISO 31000: 2018 and COSO ERM. Prevalence and suitability in enterprises

Ioannis Manoukas

Supervisor

Antonios Targoutzidis

April 2023

Open University of

Cyprus

Faculty

ECONOMICS AND

MANAGEMENT

Postgraduate Programme of Study ENTERPRISE RISK MANAGEMENT

Master Thesis

ISO 31000: 2018 and COSO ERM. Prevalence and suitability in enterprises

Ioannis Manoukas

Supervisor

Antonios Targoutzidis

April 2023

This Master's Dissertation was submitted in partial fulfillment of the requirements for the award of the postgraduate title

on ENTERPRISE RISK MANAGEMENT

by the Faculty of ECONOMICS AND MANAGEMENT

of the Open University of Cyprus.

ABSTRACT

In current extremely volatile business environment, all entities need to handle a wide range of risks that pose threat to their operations. Several risk management frameworks have been introduced to address these issues, with ISO 31000 and COSO ERM, having a holistic approach that involves all functions and levels of the enterprise simultaneously, being the most advanced and popular, currently.

Subject of this thesis is the critical evaluation of these 2 prevailing standards in risk management, as well as the field research of their prevalence and suitability in enterprises.

In the theoretic part, the study analyses the risk management concept and the two standards through a broad literature review focusing on their comparison, similarities and differences. In its main empirical part, the study investigates the characteristics of the companies (sector, size, location etc.) that determine the preference for one or the other standard.

Since neither ISO 31000, nor COSO ERM are officially certifiable and there do not exist official databases of entities that apply them, information that was indirectly derived through search in internet, management reports, press releases, articles, social media etc., concluded to a non-exhaustive dataset of 367 enterprises and organizations.

The results of statistically analyzing the above sample identify that: a) ISO 31000 is more popular around the globe, but a big percentage of entities (36.2%) chose to apply both standards, b) Size of the company is essential in the choice of the standard to follow, c) there are patterns of preference of one (or both) of the standards, related to the country of origin of the entity and d) economic sector has also an effect on the choice, with industries with more risk averse culture being those that apply both standards.

Finally, given the limitations and challenges of sampling, we suggest that future scientific research should consider: formation of an official registry of applications worldwide, investigation of additional factors that may affect the choice/preference of

a specific risk management framework and follow up of existing applications to identify potential problems encountered, variations from the authentic standard's concept, stakeholders' experience etc.

Keywords: *Enterprise Risk Management, ISO 31000, COSO ERM*

TABLE OF CONTENTS

ABBREVIATIONS

COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	Enterprise Risk Management
ISO	International Standards Organization

LIST OF DIAGRAMS

INTRODUCTION

Subject of this thesis is the critical evaluation of the two prevailing standards in risk management, namely ISO 31000 and COSO ERM, as well as the field research of their applications in companies.

The environment in which businesses operate today is particularly volatile compared to the past. Business people and managers are daily faced with a variety of risks related to both economic and political conditions, as well as the natural environment (natural disasters, floods, etc.), pandemics and geopolitical crises. Risk management theory has been a field of scientific research in recent decades that has seen great growth (Leledakis, 2007).

ISO 31000:2018 is a standard that holistically addresses risk management at all levels of the enterprise simultaneously. It allows for case-by-case management of different levels or departments of the business, but the operation remains centralized (the same processes can be applied separately at different levels or departments) with very limited flexibility.

COSO ERM, on the other hand, focuses rather on risk strategy and its alignment with core corporate values than on organizational structure. This is very important in large organizations with different entities, where flexibility is required to adapt each entity to its own operating context, while maintaining the same basic risk management principles at local and corporate level, as well as common monitoring and control.

The aim of this dissertation is to identify the prevalence of each standard in companies internationally and to investigate the characteristics of the companies (sector, size, etc.) that determine the preference for one or the other standard. Thus, the rest of its content unfolds as follows:

The first chapter refers to the basic concepts of risk management, the types of risks faced by an enterprise and the ways of analyzing and dealing with them.

Chapters 2 and 3 provide a brief description of the principles and content of the 2 standards focusing on their structure, orientation and procedures.

The fourth chapter is dedicated to the critical comparative consideration of COSO ERM and ISO 31000 analyzing their similarities and differences, while chapter 5 is dedicated to a review of recent international scientific literature and research articles, regarding their applications in various industries and enterprises, to address the question of their prevalence and adequacy for business.

In chapter 6, data and characteristics of 367 companies and organizations that have adopted one or the other standard are gathered, as they arise from official or unofficial articles, press releases, annual reports or other means. The research questions and the research methodology are also analyzed in this chapter.

Then, in chapter 7, data are processed statistically to investigate the potential existence of patterns of preferences by industry, size, organizational structure etc. the results of the research are critically considered in comparison with findings from the literature review and their commentary.

Finally, the thesis concludes in the 8th chapter, with the conclusions drawn, the existing concerns and limitations, as well as suggestions for further scientific research in the subject.

CHAPTER 1. RISK MANAGEMENT FUNDAMENTALS

1.1 Risk Types

According to the Institute of Risk Management-IRM (www.theirm.org), risk is defined as "*the combination of the probability of an event and its consequences*" When the risk is associated with favorable results, it is characterized as upside risk. Otherwise, the risk is called downside.

In international literature only cases of downside risks are analyzed, and this is rather anticipated, given that the opposite case can be more like an "opportunity" rather than a risk of losses for which the company should take appropriate measures.

In the literature, the types of risk faced by a company are distinguished into 4 major categories depending on the type of financial transaction/activity and the asset at stake:

(a) credit risk

(b) market risk

(c) liquidity risk and

(d) operational risk.

Credit risk is the risk incurred by a creditor when the borrower fails to fulfill its obligations according to the agreed terms. Three basic elements of credit risk are (Kalfaoglou, 1999):

1) default risk: failing of the borrower to keep the promise of repayment.
2) exposure risk which concerns the total amount of the portfolio that is exposed to credit risk and
3) recovery risk is the difference between the amount that is in default and the amount of the final payment.

Market risk is the risk of losses occurring in an investment due to changes in its value. This risk appears as (Van Greuning & Brajovic Bratanovic, 2017):

1) stock market risk or risk of changes in the share price,
2) interest rate risk (risk that interest rates change negatively),
3) currency risk (risk that currency rates change) and
4) commodity risk (the risk of a change in the price of commodities used to implement the investment).

Liquidity risk refers either to the ability of a company to meet its short-term obligations, or to the risk that an asset cannot be sold immediately at a price commensurate with its purchase price, due to reduced demand (Greenbaum et.al, 2019).

Finally, **operating risk** is defined as the risk faced by a company during its operation, due to inadequacy or failure of internal processes and systems, external threats resulting from catastrophic events or human errors, intentional or not (Deloitte, 2019). Operational risk is classified as pure downside risk as it always leads to a financial loss for the business. The failure to mitigate and effectively manage operational risk events in the past has led to the "annihilation" of many businesses and financial institutions (Ferreira & Dickason-Koekemoer, 2019).

1.2 Risk and Uncertainty Difference

To better understand the concept of risk, it is necessary to make a clear distinction between risk and uncertainty. Risk refers to situations in which probabilities of potential outcomes can be identified. In other words, it can be quantified.

Conversely, uncertainty refers to situations or events about which there is insufficient information to identify objective probabilities. Therefore, when the information necessary to understand and predict developments or changes that may occur in a particular context is either insufficient or unavailable, the situation is defined as uncertain.

The key to distinguishing between risk and uncertainty is probability. Probability refers to a certain phenomenon or event occurring under well-defined conditions. Depending on the probability, three categories of situations can be distinguished:

- absolute certainty,

- uncertainty,
- risk.

The state of absolute certainty implies the exact knowledge of economic phenomena and factors, as well as a strict control of the time of appearance of the resulting effects, which in mathematics is expressed by a probability of occurrence $p(x)=1$. It is a situation that is very rarely encountered in social and economic life or in nature. If there is a situation of absolute certainty, it usually happens in a relatively short period of time.

The state of uncertainty means a set of conditions and factors, undefined and unpredictable as to their appearance and development. Even if they are detected and predicted, they are extremely unstable, so they are especially difficult to express mathematically. We consider their mathematical probability $p(x)=0$.

The risk situation is when, with a probability of $0<p(x)<1$, the appearance and evolution of economic phenomena, the influence of factors that cause them and their possible effects can be determined (Toma et.al., 2012).

Uncertainty in risk management can be divided into two categories: aleatory and epistemic uncertainty (Nilsen & Aven, 2003, Yalcintas, 2013).

a. Aleatory uncertainty stems from the variance in known (or observable) quantities, which is due to random factors of the phenomenon under study. This type of uncertainty can be observed when repeating the same experiment under the same conditions and the results differ.

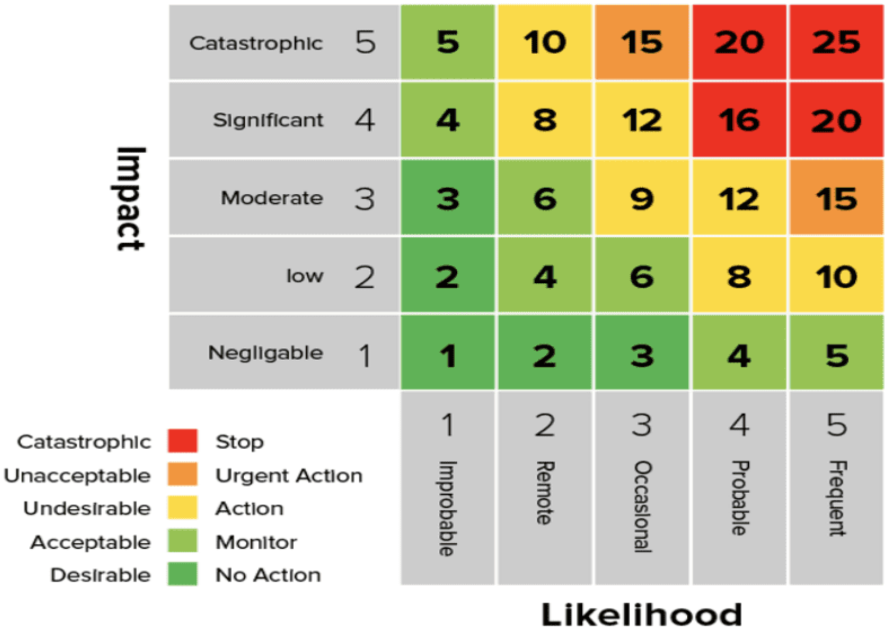
b. Epistemic uncertainty stems from the lack of knowledge about the phenomenon under study (for example the case of "black swans"). The specific uncertainty can be reduced by improving the knowledge on the subject under study (Aven, 2015).

1.3 Risk measurement and heatmaps

Risk is measured by the likelihood and the size of the impact of the event. Expressed mathematically, risk equals anticipated damages multiplied by their likelihood. For risk prevention and management professionals, the goal is to find occurrence criteria and to determine the probability of the event (Beasley et.al., 2010). When the result of this equation is a low value, because either the probability of the event or the severity of the damages is low, the risk is considered negligible.

A risk heat map is a tool often used to present the results of a risk assessment process visually and in a meaningful and concise way. The development of an effective heat map has several critical elements – a common understanding of the risk appetite of the company, the level of impact that would be material to the company, and a common language for assigning probabilities and potential impacts (CGMA, 2013).

Diagram 1.1: Risk level heatmap



Impact	Catastrophic	5	5	10	15	20	25
	Significant	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	low	2	2	4	6	8	10
	Negligable	1	1	2	3	4	5
			1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
			Likelihood				

Catastrophic	🟥	Stop
Unacceptable	🟧	Urgent Action
Undesirable	🟨	Action
Acceptable	🟩	Monitor
Desirable	🟩	No Action

Source: CGMA, 2013

Organizations generally map risks on a heat map using a '**residual risk'** basis that considers the extent to which risks are mitigated or reduced by internal controls or other risk response strategies. In addition, it is often considered an 'acceptable" risk, that the organization is prepared to tolerate from an economic point of view, taking into account the current knowledge about the risks in a given situation.

1.4 Risk analysis and management

Each organization should determine the level and type of risk it can or cannot take, in relation to its goals. It should also define criteria for assessing risk severity and supporting decision-making processes. Risk criteria should be aligned with the risk management framework and adapted to the specific purpose and scope of each activity under consideration. At the same time, risk criteria must reflect the organization's values, goals and resources, be consistent with risk management policies and be measurable.

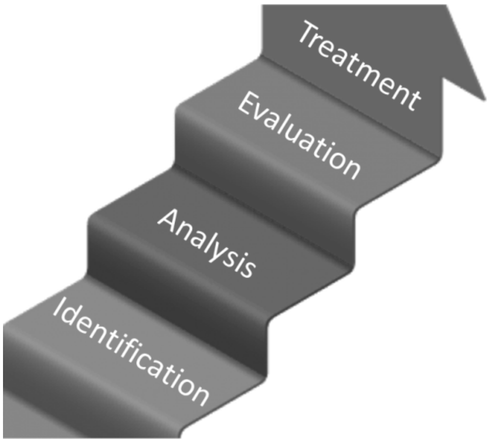
The risk management process includes 4 steps: a) Risk identification, b) risk analysis, c) risk assessment, d) risk treatment.

Risk identification refers to the identification of the following factors that can cause risk:

- tangible and intangible sources of risk
- causes and events
- threats and opportunities
- vulnerabilities and capabilities
- changes in the external and internal environment
- indications of emerging risks
- nature and value of assets and resources
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information
- factors related to time,

- prejudices, assumptions and beliefs of those involved.

Diagram 1.2: Phases of Risk Management



Risk analysis is concerned with the investigation of factors such as:

- the probability of events and consequences,
- the nature and magnitude of the consequences,
- difficulty of management,
- factors related to time,
- the effectiveness of existing controls,
- levels of sensitivity and assurance.

Risk assessment leads to decisions such as:

- No further action,
- examination of the options for dealing with the risk,
- further analysis to better understand the risk,
- maintenance of existing controls,
- review of objectives.

Risk treatment involves an iterative process of:

- formulation and selection of risk treatment options:
    - avoiding the risk by deciding not to start or continue the activity that creates the risk.
    - taking or increasing risk in pursuit of an opportunity;
    - removal of the source of danger,
    - changing the probability by taking action,
    - changing consequences by taking action;
    - risk sharing (e.g., through contracts, purchase of insurance, etc.);
    - maintaining risk with an informed decision.
- design and implementation of risk treatment,
- evaluation of the effectiveness of this treatment with regular reviews and reports for decision-making,
- decision whether the residual risk is acceptable,
- use of further treatment if the level of residual risk is not acceptable.

1.4. Risk Management Standards

In the last 20 years, the knowledge of companies regarding the relationship between risks, objectives and efficiency has gradually increased. As a result, the sensitivity for the right holistic approach to the management of the risks they face both at a strategic and operational level increased as well.

This management is usually referred to as "Integrated Risk Management -IRM or Enterprise Risk management-ERM" and is the subject of continuous research and improvement both by the scientific community and by the control, regulatory and supervisory mechanisms at an international level (Bosetti, 2015).

As a result, many national and global standards, regulations and guidelines have been issued by various organizations. The adaptation of companies to these standards is usually done on a "voluntary" basis, in the context of the application of best practices, but in several cases, it has become mandatory, especially in sensitive sectors of the economy (e.g., banks and credit institutions).

Such standards of integrated risk management at an international level are:

- COSO ERM Integrated Framework (from the Committee of Sponsoring Organizations).
- ISO 31000 ERM Framework (from the International Organization for Standardization).
- FERMA Risk Management Standard (from the Federation of European Risk Management Associations).
- OCEG Red Book 3.0 Governance, Risk and Compliance Capability Model (OCEG is a global nonprofit organization and community specialized in GRC standards)

At the national level there are also mandatory standards, in several cases, as for example (Bosetti, 2015, Haddad & Laghzaoui, 2020):

- The UK Financial Reporting Council's FRC Guidance on Risk Management, for companies listed on the London Stock Exchange.
- CAN/CSA Q850 in Canada, which in its most recent version is a copy of ISO 31000.
- AS/NZS 4360 Risk Management in Australia and New Zealand

Especially for the banking industry, the most influential are the standards and directives of the Basel Committee (Basel, 2001, 2004 & 2010), which have been adopted by the European Central Bank and by extension by all the banks of the Eurozone, but also from other countries.

Finally, for the operation and risk management of information systems, specialized standards have been issued, such as:

- The COBIT ERM Framework of the Information Systems Audit & Control Association (ISACA)

- The NIST ERM Framework of the US National Institute of Standards and Technology for cybersecurity (NIST, 2012 &2018).

In addition to the above, many other standards have been issued on a case-by-case basis, resulting to a sincere confusion about approaches and methodologies, which probably cause more mistrust and skepticism in the business world, since they often differ significantly even in the definition of risk, let alone in their methodological frame.

These phenomena tend to disappear in the last 5 years, after the publication of COSO ERM and ISO 31000, when a gradual convergence and adaptation of all other standards to these two comprehensive standards is observed (Haddad & Laghzaoui, 2020).

1.5 Skepticism about Enterprise Risk Management

Applications of ERM standards are various and diverse in enterprises worldwide. Nevertheless, several economists and executives are still skeptical whether ERM adds value since modern portfolio theory argues that shareholders can without much cost eliminate risks through portfolio diversification. It is therefore argued that any expenditure to mitigate firm-specific risks, including the costs associated with a risk management function and ERM initiatives, is therefore a negative net present value investment (Mikes & Kaplan, 2015).

Pagach and Warr (2010) studied ERM’s effect on long-term performance in 106 firms, mostly in the financial and utility industries, that announced the appointment of a chief risk officer (CRO). Finding no significant changes in various firm performance variables and mainly stock price data, they conclude that ERM did not add value.

In the same line, González et.al. (2020) evaluate the effect of ERM on the performance and the financial stability of a sample of non-financial Spanish listed companies, based on information derived from annual reports, management reports and annual corporate governance reports between 2012 and 2015. Their results show that the adoption of ERM was not associated with a change in ROE or ROA of the companies nor did it reduce the probability of bankruptcy. The researchers, rather anti-mainstream, conclude that having a chief risk officer (CRO) can actually reduce performance, although it can improve the degree of financial health measured as the distance to default.

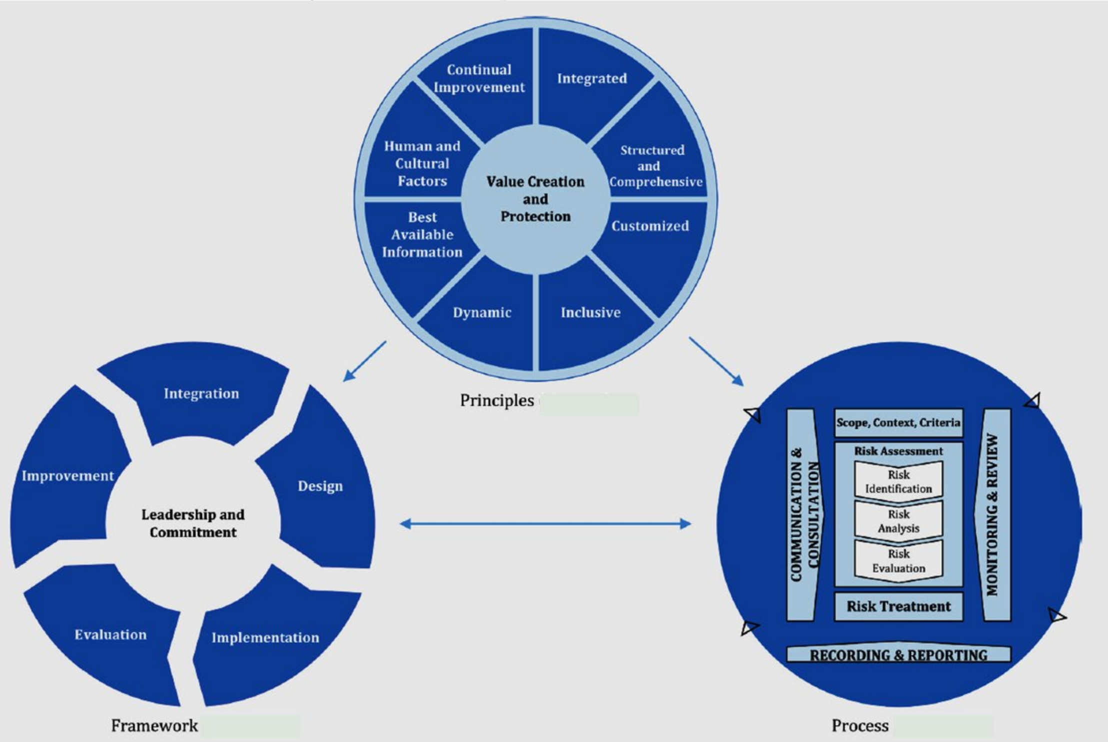
CHAPTER 2. ISO 31000 STANDARD

2.1 The Standard

“ISO 31000:2018 Risk Management-Guidelines” is a standard developed and published by the International Organization for Standardization (ISO[1]). Its aim is to offer guidelines for adopting effective risk management activities and processes in all types of organizations (It isn't specific to any industry or sector) - for example, equipment failure, employee or customer accidents, cybersecurity breaches and financial fraud.

ISO 31000 consists of three core elements for risk management: Principles, Framework, and Process (Diagram2.1).

Diagram 2.1: Principles, Framework and Process



Source: ISO 31000:2018

[1] The International Organization for Standardization (ISO) is a worldwide independent, nongovernmental federation of national standards bodies (ISO member bodies) with a current number of 165 members. It was founded in 1947 to develop and publish standards for companies and other entities worldwide and up to date, it has developed nearly 24,000 international standards for management systems, quality management, occupational health and safety, information security and many other topics, including risk management. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The standard was first released in 2009 and then revised in 2018 The updated version offers a shorter, clearer and more concise view on Enterprise Risk Management (ERM) than the previous one.

To reduce the amount of specific terminology in ISO 31000, some terms were moved to ISO Guide 73[2], a risk management vocabulary document that's meant to be used with the standard. In addition, ISO 31000:2018 provides more strategic guidance on ERM than the original standard "*and places more emphasis on both the involvement of senior management and the integration of risk management into the organization*," according to ISO.

The English version of ISO 31000, from where the majority of information in this chapter has been derived, is available for free at iso.org[3]. Text straight derived from the body of the standard's document is marked in italic fonts.

A complementary standard to ISO 31000:2018 is IEC 31010:2019 standard[4] on risk assessment and analysis techniques. It is jointly developed by ISO and the International Electrotechnical Commission, although it's published under the IEC's name.

Moreover, based on ISO 31000, the ISO 27005:2022 standard is about Information Technology- Information security risk management.

2.2 Terminology

Risk *Effect of uncertainty on objectives.*

Consequence *Outcome of an event affecting objectives.*

A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Consequences can be expressed qualitatively or quantitatively.

[2] https://www.iso.org/standard/44651.html (last visit 31/3/2023)

[3] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en (last visit 31/3/2023)

[4] https://www.iso.org/standard/72140.html (last visit 31/3/2023)

Any consequence can escalate through cascading and cumulative effects.

Control *Measure that maintains and/or modifies risk.*

Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Controls may not always exert the intended or assumed modifying effect.

Effect *A deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.*

Event *Occurrence or change of a particular set of circumstances.*

An event can have one or more occurrences and can have several causes and several consequences.

An event can also be something that is expected which does not happen, or something that is not expected which does happen.

An event can be a risk source.

Interested Party *Stakeholder*

Likelihood *Chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).*

Objectives *Objectives can have different aspects and categories and can be applied at different levels.*

Risk management *Coordinated activities to direct and control an organization with regard to risk*

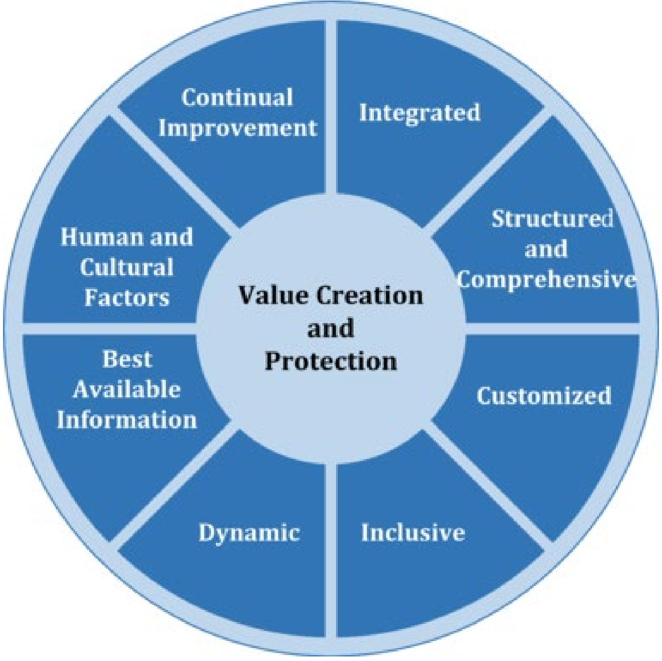
Risk source *Element which alone or in combination has the potential to give rise to risk*

Stakeholder *Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity*

2.2 ISO 31000 Principles

ISO 31000 lists eight principles (Diagram 2.2) as the foundation for managing risk to create and protect business value. They provide guidance on the characteristics of effective and efficient risk management efforts and on how to explain the purpose of ERM and communicate its value.

Diagram 2.2: ISO 31000 Principles


Continual Improvement
Integrated
Human and Cultural Factors
Structured and Comprehensive
Value Creation and Protection
Best Available Information
Customized
Dynamic
Inclusive

According to ISO, these principles are explained as follows:

1) ***Integrated:*** Risk management is an integral part of all organizational activities and it should be comprehensively integrated into an organization's decision-making processes.

2) ***Structured and comprehensive:*** A structured and comprehensive approach to risk management is required for consistent and comparable results.

3) ***Customized:*** All organizations are different in structure and operations. The risk management framework and process should be customized and proportionate to the organization's external and internal context and to its objectives.

4) ***Inclusive:*** Active and timely involvement of internal and external stakeholders enables diffusion of expert knowledge, views and perceptions. This leads in improved awareness and informed risk management.

5) ***Dynamic:*** As business environment dynamically changes, new risks emerge and existing change or disappear. Risk management anticipates, detects, acknowledges and responds to those changes, in an appropriate and timely manner.

6) ***Best available information:*** Inputs to risk management are based on best available information as historical and current data, future expectations, experts' judgement. Risk management explicitly considers any limitations of available information*. Information should be timely, clear and available to relevant stakeholders.*

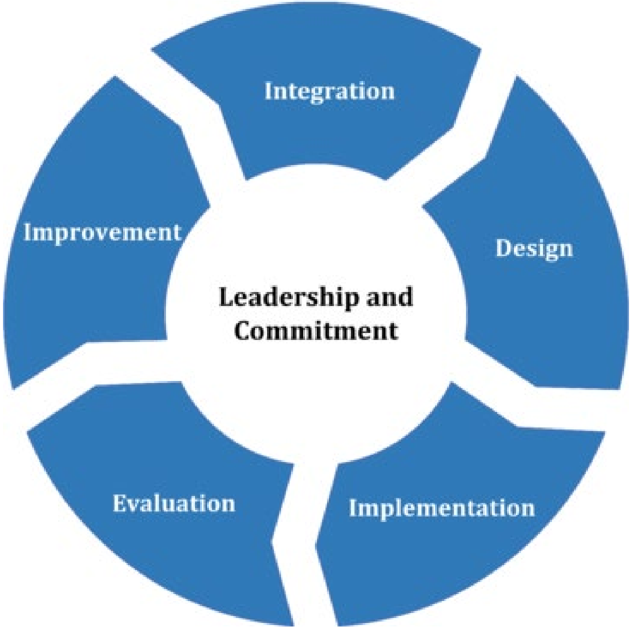
7) ***Human and cultural factors:*** Human behavior, cultural factors and management team's attitudes towards risks and risk management greatly influence all risk management.

8) ***Continual improvement:*** Risk management is iterative and facilitates continual improvement of the organization, through learning and experience.

2.3 ISO 31000 Framework

This is designed to help organizations apply risk management mechanisms in business functions and governance structures. It includes six customizable components (Diagram 2.3):

Diagram 2.3: ISO 31000 Framework



1. **Leadership and commitment:** *Top management and/or management bodies, should ensure that risk management is integrated into all organizational activities.*

2. **Integration:** *Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations.*

3. **Design:** *When designing the framework for managing risk, top management and oversight bodies, where applicable, should:*

   a. *examine and understand its external and internal context,*

   b. *demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management,*

   c. *assign organizational roles, authorities, responsibilities and accountabilities with respect to risk management,*

   d. *Top management and oversight bodies, where applicable, should ensure allocation of appropriate resources for risk management,*

e. *establish an approved approach to communication and consultation in order to support the framework and facilitate the effective application of risk management.*

4. **Implementation:** *The organization should implement the risk management framework by developing an appropriate plan including time and resources, modifying the existing decision-making processes where necessary and ensuring that the organization's arrangements for managing risk are clearly understood and practiced by all stakeholders.*

5. **Evaluation:** *Periodical evaluation of measure risk management framework performance against its purpose, implementation plans, indicators and expected behavior to determine whether it remains suitable to support achieving the objectives of the organization.*

6. **Improvement:** *Continually monitor and adapt the risk management framework to address external and internal changes, improve its suitability, adequacy and effectiveness and the way the risk management process is integrated.*

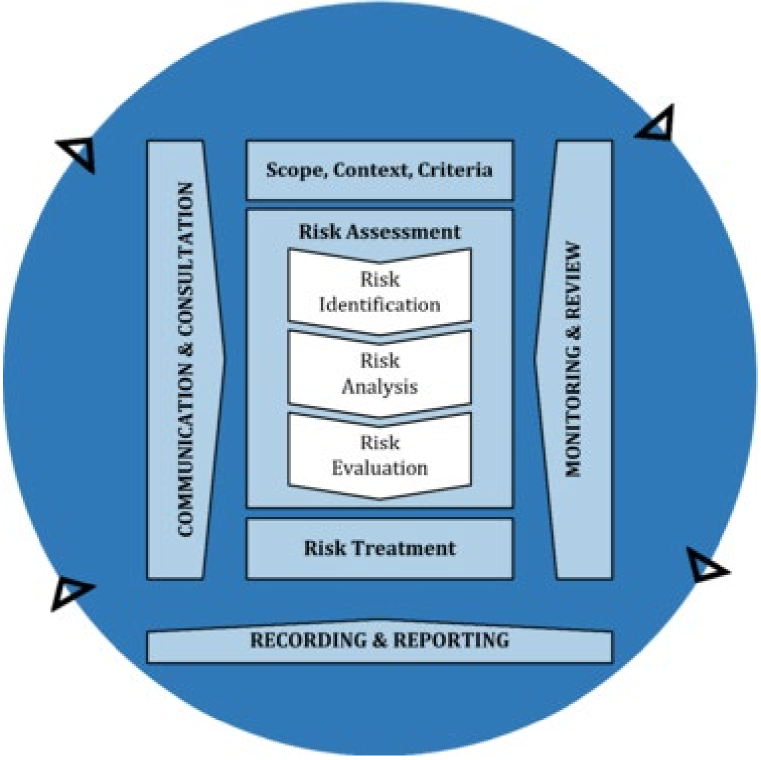
2.4 ISO 31000 risk management process

The standard outlines the process that organizations should use to identify, evaluate, prioritize and mitigate risks, with guidance on how to apply policies, procedures and practices in a systematic way. It also includes steps for communication, monitoring and review, and reporting. It is moted that the risk management process is often presented as sequential, in practice it is iterative.

Risk assessment and **Risk treatment** pillars are as described in paragraph 1.3.

The purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Defining the scope is important in aligning the process objectives with the overall organizational objectives. The context of the risk management process refers to the external and internal environment in which the organization operates and should reflect the specific environment of the activity to which the risk management process is to be applied. The organization should specify the amount and type of risk that it may *or may not take, relative to objectives and it should also define criteria to evaluate the significance of risk and to support decision-making processes. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope of the activity under consideration. Moreover, they should reflect the organization's values, objectives and resources and be consistent with policies and statements about risk management.*

Diagram 2.4: ISO 31000 Risk Management Process



Continuous and uninterrupted communication and consultation with appropriate external and internal stakeholders during the risk management process is essential to assist in understanding risk and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining expertise feedback and information to support decision-making.

Ongoing monitoring and periodic review in all stages of the process and its outcomes should be a planned part of the risk management process, with responsibilities clearly *defined. Their outcomes should be incorporated throughout the organization's performance management, measurement and reporting activities.*

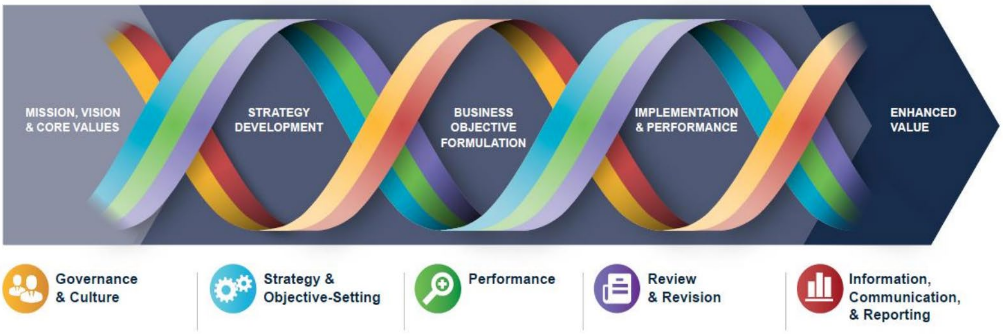
CHAPTER 3. COSO ERM FRAMEWORK

3.1 The Standard

“COSO Enterprise Risk Management -- Integrating with Strategy and Performance" is a framework for enterprise risk management issued by the Committee of Sponsoring Organizations (COSO[5]). Its aim is to address the increasing complexity of ERM and the corresponding need for organizations to improve the way they manage risk to meet changing business demands. It can be used (like ISO 31000) in organizations of all sizes and in all industries.

It was first released in 2004 and then revised in 2017. The updated version, compared to the previous one, highlights the importance of considering risk in setting business strategies and managing operational performance. According to COSO, the 2004 version still remains valid and complimentary to the new one.

Diagram 3.1 Enterprise Risk management as per COSO


MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

Source: https://www.coso.org/COSO-ERM-Presentation-September-2017.pdf

COSO ERM Framework includes altogether more than 100 pages of text and visual elements. The majority of information in this chapter has been derived from its official

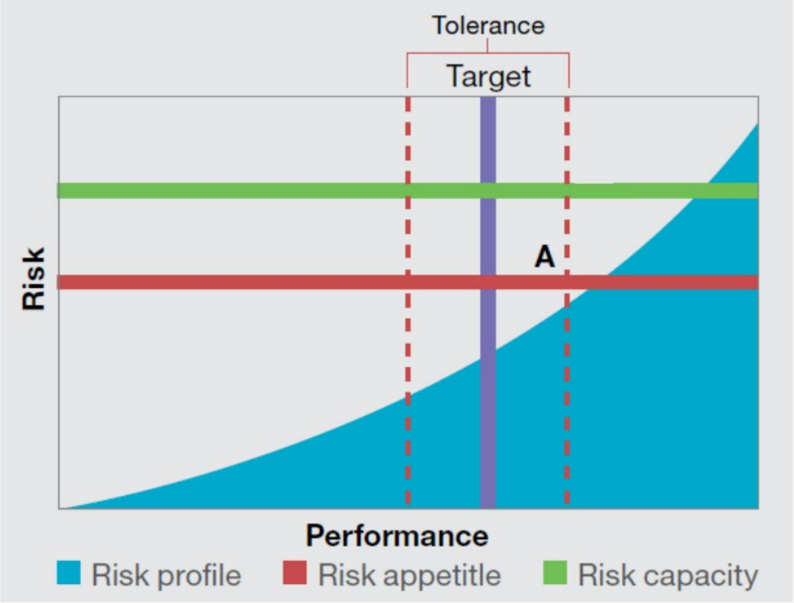
[5] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private sector initiative in US, founded in 1985 jointly by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors and the Institute of Management Accountants. Its name refers to its first president James C. Treadway, Jr., a former Commissioner of the US Securities and Exchange Commission. The Committee’s mission is to “help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence” and its output includes standards frameworks, research studies and thought papers.

executive summary (COSO, 2017). Text straight derived from the body of the standard's document is marked in italic fonts.

3.2 COSO ERM Approach to Risk

COSO ERM introduces a new depiction referred to as a risk profile, which according to COSO offers a comprehensive view of risk and enables more risk-aware decisions. Risk profile incorporates (Diagram 3.2):

Diagram 3.2: Enterprise Risk Profile in COSO ERM



Source: https://www.coso.org/COSO-ERM-Presentation-September-2017.pdf

- **Risk:** the possibility that events will occur and affect the achievement of strategy and business objectives.

- **Performance:** Enterprise risk management performances (ie identifying, assessing, prioritizing, responding to, and developing a portfolio view of risk) that support the organization's decisions in its search of value.

- **Risk appetite:** The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. The notion of risk appetite is central in COSO ERM and it can be objectives-based or risk-based (COSO, 2020a).

- **Risk capacity:** the maximum amount of risk that a firm can take before the firm fails should those risks are realized.

- **Risk tolerance:** it reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve. Risk tolerance is the level of risk that an organization is willing to accept per individual risk.

Moreover, COSO ERM builds links to internal control and complements the "COSO Internal Control – Integrated Framework", some aspects of the latter being further developed in ERM Framework.

3.3 COSO ERM Framework

COSO ERM Framework is a set of 20 principles that describe the specific actions and practices required and are organized into five interrelated components:

1. **Governance and culture:** Risk governance and culture together form a strong foundation for the ERM and basis for all other components. *Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.*

    i. *Exercises Board Risk Oversight—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.*

    ii. *Establishes Operating Structures—The organization establishes operating structures in the pursuit of strategy and business objectives.*

    iii. *Defines Desired Culture—The organization defines the desired behaviors that characterize the entity's desired culture.*

    iv. *Demonstrates Commitment to Core Values—The organization demonstrates a commitment to the entity's core values.*

    v. *Attracts, Develops, and Retains Capable Individuals—The organization is committed to building human capital in alignment with the strategy and business objectives.*

2. **Strategy and objective-setting:** Setting strategy and business objectives are the key activity of an Organization and the ERM has to be integrated at this level. This gives organization an insight into internal and external factors and their impact to risk. An organization sets its risk appetite in conjunction with strategy-setting. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.

   i. *Analyzes Business Context Context—The organization considers potential effects of business context on risk profile.*

   ii. *Defines Risk Appetite—The organization defines risk appetite in the context of creating, preserving, and realizing value.*

   iii. *Evaluates Alternative Strategies—The organization evaluates alternative strategies and potential impact on risk profile.*

   iv. *Formulates Business Objectives—The organization considers risk while establishing the business objectives at various levels that align and support strategy.*

3. **Performance:** *Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.*

   i. *Identifies Risk Risk—The organization identifies risk that impacts the performance of strategy and business objectives.*

   ii. *Assesses Severity of Risk—The organization assesses the severity of risk.*

   iii. *Prioritizes Risks—The organization prioritizes risks as a basis for selecting responses to risks.*

   iv. *Implements Risk Responses—The organization identifies and selects risk responses.*

v. *Develops Portfolio View—The organization develops and evaluates a portfolio*

4. **Review and revision:** *By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.*

   i. Assesses Substantial Change—The organization identifies and assesses changes that may substantially affect strategy and business objectives.

   ii. Reviews Risk and Performance—The organization reviews entity performance and considers risk.

   iii. Pursues Improvement in Enterprise Risk Management—The organization pursues improvement of enterprise risk management.

5. **Information, communication and reporting:** *Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.*

   i. Leverages Information Systems—The organization leverages the entity's information and technology systems to support enterprise risk management.

   ii. Communicates Risk Information—The organization uses communication channels to support enterprise risk management.

   iii. Reports on Risk, Culture, and Performance—The organization reports on risk, culture, and performance at multiple levels and across the entity.

The principles can be applied in different ways by different organizations. As further guidance on that, COSO has also published a "Compendium of Examples" supplement with case studies on implementations of the ERM framework by individual entities.

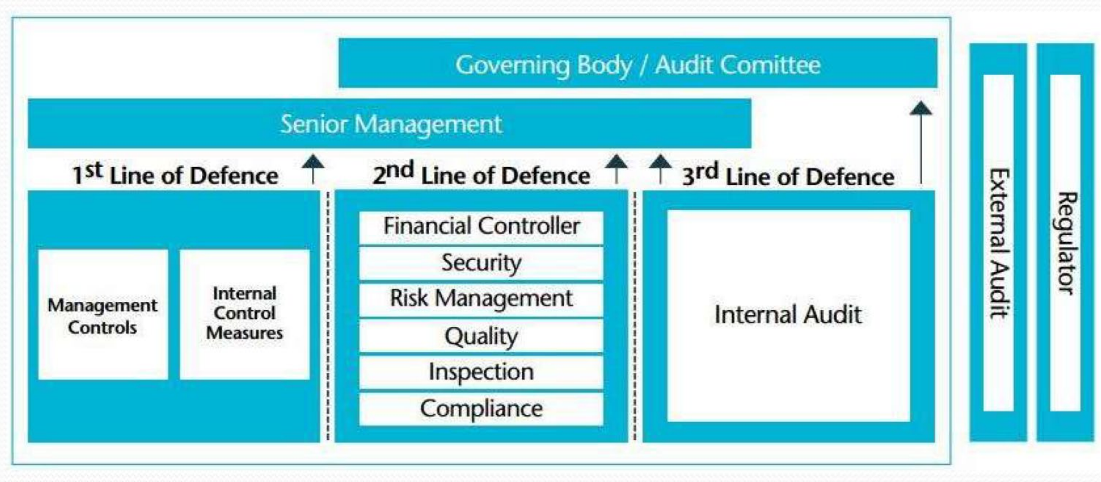
3.4 Three Lines of Defense Structure

The goal of any organization is to achieve its business objectives. In that effort, it needs to create the right organizational structure that can facilitate taking the appropriate risks and managing them. Such structure is the “Three Lines of Defense” model, which helps segregating the roles and responsibilities of the stakeholders (Diagram 3.3).

In the Three Lines of Defense model, front line management is the first line of defense, risk management and compliance functions are the second line of defense, and Audit and independent assurance is the third line.

Neither governing bodies nor senior management are part of three "lines" of defense. Instead, governing bodies and senior management are the primary stakeholders served by the three lines (Kumar, 2022).

Diagram 3.2: Three Lines of Defense Structure



Source: Kumar, 2022.

<u>First Line of Defense</u>

The first line of defense is the business and process owners who facilitate the achievement of business objectives by managing risks. This includes taking the right risks. The first line owns the risk, design, and execution of the organization's controls to respond to those risks. The first line is responsible for:

a. Day-to-day risk management decision making

b. Risk identification, assessment, mitigation, monitoring, and management

c. Effective implementation of the risk management framework

d. The first line of defense examples are Sales, Marketing, Finance, Operations, Investments, Strategy, HR, etc.

Second Line of Defense

The second line of defense is the risk and compliance functions. The second line of defense functions are separate from the first line of defense but are still under the control and direction of senior management. The second line is essentially an oversight function that owns many aspects of the management of risk. Examples of Second Line of defense are

- Risk Management
- Information Security
- Physical Security
- Quality
- Health and Safety
- Compliance etc

Third Line of Defense

The third line of defense is the Internal Audit team, that has the obligation to review appropriateness, effectiveness, and adequacy of the risk management framework and assure senior management and the Board over both the first and second lines' efforts.

CHAPTER 4. CRITICAL COMPARISON OF THE TWO STANDARDS.

As mentioned in Chapter 1, there have been many different Risk Standards issued worldwide in the previous decades. Yet after the updates of ISO 31000 and COSO ERM Framework in 2018 and 2017 respectively, it seems that they prevail and encompass all previous efforts. Therefore, the critical comparison between the two is inevitable for the researcher who tries to conclude to the best practice approach.

Several similar attempts have been carried out in the previous 5 years. For example, one can mention the IRM's Risk Practitioner's guides to COSO ERM and ISO 31000, scientific articles (Rubino, 2018; Hamir & Sum, 2021; Læssøe, 2022), as well as critical reviews in well-respected risk management or technological sites like techtarget.com, intermediate.pro, learn31000.com, reciprocity.com, erminsightsbycarol.com, riskpublishing.com.

4.1 COSO ERM & ISO 31000 Similarities

ISO 31000 and COSO's ERM framework have the same ultimate goal: helping organizations to implement effective risk management strategies and processes. Here are some similarities between the two standards that risk management experts and software vendors commonly cite:

- ISO 31000 and COSO both broaden the scope of risk management. They view it as more than minimizing negative risks and they encourage taking right risks to achieve objectives.

- They are both guidelines for organizations, and there is no certification or mandatory compliance associated with either of them. Under each standard, an ERM system needs to be customized to the individual organization, and the guidelines can be adapted as needed to accomplish that.

- Both ISO 31000 and COSO focus on techniques and methods used to evaluate, manage and monitor risks. In many ways, they're representations of the same body of knowledge.

- Both ISO 31000 and COSO embed risk management into an organization's decision-making processes so corporate executives and business managers understand the risks and how they relate to organizational objectives when they make business decisions. Yet, although each standard mentions the importance of factoring risk into the decision-making process, both ignore decision-making science altogether.

- Both emphasize the need to review risks and revise ERM strategies and controls as new business issues and requirements emerge.

- The two standards were both dramatically updated from their previous versions at about the same time to make it easier to understand and implement them.

4.2 COSO ERM & ISO 31000 differences

There also are many differences between ISO 31000 and the COSO ERM framework. These are some typically listed by experts and vendors:

1. **Formation:** ISO 31000 is rather structured and just 16 pages (although it is supplemented by the vocabulary guide and IEC 31010). COSO ERM framework is extensive including more than 100 pages of text and visual elements.

   ISO 31000 is easier to understand and contains descriptions of risk management steps plus practical advice on how risk management should be integrated into decision-making processes. COSO is multilayered and complicated, however it includes ideas and advice that can be used to supplement the briefer ISO guidance plus COSO has also released documents on applying it to specific areas, such as cloud computing and managing compliance risks.

2. **Completeness:** COSO is completer and more comprehensive, especially if carried out jointly with its 2004 version that still remains valid (Rubino, 2018).

3. **Development:** ISO 31000 is developed by a formal standards body, and ISO received more than 5,000 comments from people in 70+ countries when it was working on the 2018 version. COSO, on the other hand, is a group of

professional associations, and the 2017 ERM framework update was developed by consulting firm PwC with direction from COSO's board and input from external "advisors and observers."

4. **Geographical Scope:** ISO 31000 is the official ERM standard for organizations in about 70 countries. Most of the parties that have made an important contribution to COSO ERM are located in the United States, where COSO has its own merits and legacy.
5. **Focus.** The COSO framework focuses more on general enterprise-level governance and auditing of risk management activities, providing a standard against which to evaluate an organization's current ERM practices. ISO 31000 focuses squarely on risk management and its role in strategic planning and decision-making, providing guidance on the nature of the ERM and how it can be applied to any type of risk (Rubino, 2018).
6. **Target Audience.** Being a more generic risk management standard, ISO 31000 is written for a broad audience of people interested in ERM. COSO ERM mainly targets people and organizations in fields such as auditing and accounting.
7. **Framework, principles and process.** COSO combines its framework, principles and process into a single structure that incorporates risk management into a broader set of organizational governance and management program. ISO 31000 distinguishes between those three elements and more directly details the required risk management tasks (Hamir & Sum, 2021).
8. **Process Start:** ISO 31000 begins the risk process by defining the purpose and scope of risk management activities. The design process notes the value of scope and purpose in establishing risk criteria and decision making. However, ISO 31000, while focusing on leadership commitment, considers management’s business concerns after determining risk tolerance. COSO, on the other hand, starts the risk process by reviewing the organization’s business strategies and aligning risks to those objectives. With this in mind, COSO provides a more meaningful approach to defining the risk tolerance.

Beginning with the organization's business objectives allows the c-suite to understand the risk mitigation strategies better.

9. **Risk definition:** As per COSO Risk is "*the possibility that events will occur and affect the achievement of strategy and business objectives*" (COSO, 2020b) and as per ISO Risk is "*the effect of uncertainty on objectives*".
10. **Risk appetite vs. risk criteria.** The COSO framework includes the concept of an organization's risk appetite, which it discusses in detail along with the related notions of risk tolerance and capacity. The 2018 version of ISO 31000 uses risk criteria to describe the amount and type of risk that an organization is willing to take, while it briefly mentions risk appetite, using different terminology[6].
11. **Risk reduction vs. business success.** There's no longer as much of a difference on this in the updated standards. But the COSO framework is generally seen as being centered on avoiding or minimizing risk, while ISO 31000 is oriented more toward using risk management to generate business value[6].
12. **Updates:** ISO commits to updating guidance every 5 years[7]. COSO has tended to get around to updates once a decade or longer.

[6] ISO 31000 vs COSO Enterprise Risk Management Standards (learn31000.com) [Last visited 31/3/2023]

[7] Guidance on the systematic Review Process in ISO https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100413.pdf [Last visited 31/3/2023]

CHAPTER 5. LITERATURE REVIEW.

In the last decade, the world has experienced a number of crises either economic, political or pandemic. Attempts to harmonize risk management practices in organizations internationally have been actualized in a number of risk management practices, the latest of which are COSO ERM and ISO 31000. To this end, several applications of the two frameworks have been referred in the recent scientific literature, entailing the issues raised as well as the lessons learned per case.

5.1 ISO 31000 applications

Starting with ISO 31000 applications, one should refer first to banking sector. This is because banks have quite a long tradition in risk management being the first industry to adopt scientific approaches to it. The reliable banking site "Central Banking Journal and Directory" (www.centralbanking.com/ benchmarking/risk-management) for its 2023 Benchmarking Risk Management Report interviewed officials at 32 central banks which approaches to risk management have been most influential. ISO 31000 and COSO-ERM were identified as influencing approaches by 91% and 75% of officials at central banks, respectively. Of course, European Banks follow the mandates and directives of EU that are based on the Basel Committee's framework (see Chapter 1), yet there are several applications of ISO framework in other countries over the globe. Examples may be derived from Tumenbayeva & Zhaksybekova (2016), Suyasa & Legowo (2019), Norlita & Rarasati (2019), Safitri & Pangeran (2020), Tjahjono et.al. (2022). The outcome of these studies shows that implementation of ISO 31000 assists banks to manage in a systematic and comprehensive manner diverse types of risk by providing clear steps and stages in the Risk Management process from context consideration to risk analysis, assessment and treatment.

A recent study tried to identify the problems faced by Indonesian fintech lending companies in implementing ISO 31000 (Alijoyo, 2022). Specifically, the research aimed at the responses of the managements through questionnaires and interviews and results showed that most of the companies' management believed that they had no significant problems implementing ISO 31000:2018. In addition, they felt that implementing ISO 31000:2018 as ERM gave many benefits in running the companies.

Dias (2018) examines a case study about the applicability of ISO 31000 in the Portuguese Municipality of Maia near Porto. A great part of Portuguese municipalities is already implementing IFRS and ISA-audit for disclosing the financial statements in the global market and Maia municipality has additionally implemented ISO 9001, ISO 14001 and ISO 18001. The project was based on the integrated anti-corruption Risk Management Model for the Portuguese Public Sector and the overall objective was to design an integrated risk management model with the following objectives: a) to develop a risk management model based on ISO 31000 integrating it into the Management System based on ISO 9001, b) to assess the operationalization of the Risk Management Plan designed for corruption and related infractions and ascertain its contribution to management and c) to contribute to the continuous improvement of the management system of the municipality, placing it above its peers' level. As a final result the author concludes that: (i) a favorable corporate culture, characterized by a clear involvement of top management across the whole process is an essential condition for the consolidation of risk management and (ii) risk, if duly and well seized, in any organization either public or private, may become an opportunity to better face the future.

Alijoyo and Norimarna (2021) conducted an ISO 31000 based risk management maturity assessment in a large State-Owned Enterprise (SOE) in Indonesia in order to assist the organization to map out its pathway in building resilience and sustainability, after the Covid-19 pandemic. The SOE serves public interests in the energy sector. Meanwhile, the Ministry of Indonesian State-Owned Enterprises (MSOE) since 2011 imposed SOEs to implement ISO 31000 from its previous version. However, results are hardly observed as the implementation was driven more by compliance spirit and ad-hoc base than by the indigenous need to make a SOE sustain operationally and strategically. The research methodology used document reviews, questionnaires, focused group discussions, interviews and field research. The assessment produced a risk management maturity score of 1.62/5.00, a level indicating substantial lack of resiliency and sustainability attributes. Therefore, a 5-year road map to succeed an overall 4.00/5.00 was defined, well accepted by the BOD and incorporated in their organization's business transformation program. It was also realized that the SOE should adopt asap ISO 22301 for Business Continuity Management (BCM), which would fit in pair to the existing ISO 31000 risk management maturity road map. And would help them assure that their risk management practice has a systematic and regularly tested business recovery strategy and procedures, including business continuity and disaster recovery plans. As a case study, however, we note some shortcomings of generality and comparability. Further similar research is recommended with more SOEs as the object of study.

Govender (2018) explores the use of the risk management standard ISO 31000 by private security companies in South Africa. South Africa, since the fall of apartheid is experiencing an increasing level of crime, violence, corruption and state capture allegations, which are drivers for increased corporate governance, especially for security sector. Semi-structured interviews were conducted with security practitioners and the study found that security risk management maturity was lagging behind the standard.

In the tour and travel industry, a risk management design based on ISO 31000 is effective for identifying, analyzing, evaluating, and handling all 5 types of inherent risks (financial, operational, environmental, competitive and economic) (Asmarawati & Pangeran, 2021), It is noted that ISO has issued the ISO 31030:2021 Guidance for Travel risk management of organization and its travelers, but the standard does not apply to tourism and leisure-related travel, except in relation to travelers travelling on behalf of the organization. as a result of undertaking travel.

As Lalonde & Boiral (2012) point out the generic nature of the ISO 31000 standard helps to better identify and manage a variety of risks including threats to the environment, public health and food safety issues, threats to critical infrastructure, hazards presented by certain products, and interruption of the supply chain. This diversity of risks tends to broaden the scope of the standard’ s applicability to a wide range of situations and organizations. On the other hand, Purdy (2010) underlines that ISO 31000 does succeed in integrating into a single concise and practical model a considerable amount of knowledge accumulated from research on multiple aspects of the field which is widely scattered in the literature and thus difficult to take into account.

Other applications of ISO 31000 extracted from recent scientific literature include:

- heavy machinery vehicle operations (Wicaksono, 2019), where the aim of the research was to observe level of effectiveness in applying ISO 31000:2018 by expert judgment in risk assessment techniques using questionnaires. The operation of heavy machinery vehicles in extensive project sites and transporting of these heavy machinery vehicles from one project location to another using low bed movers imply that several business risks are likely to occur which can disrupt the course of the company's business processes and can directly reduce the profit. Twenty risks were identified and based on the results of the risk assessed from probability and impact variables, mitigation strategies were introduced. These are: avoided risk, risk control, separating risk, moving risk and accepting risk. Outcomes based on mitigation duration and mitigation costs were also assessed to find out the most optimal strategy for dealing with each of these risks.

- a group of companies that consists of 5 firms that work in construction and procurement services (Syahputri & Kitri, 2020), to find out and assess the uncertainties that occur, including operating risk, market risk and other risks.

- a pharmacy in Indonesia (Nugroho & Pangeran, 2021), where the standard's risk assessment methodology was used to identify risks like financial, operational, technology, business ethics, health and safety, economic, legal, political, market, and project risk. Based on the results of the analysis, the highest risk was evaluated to be technology risk, followed by economic risk and political risk. Recommendations were made for the treatment of each serious risk, based on the owner's risk appetite and finally a map of risk residuals was filled. This map was incorporated in a Balanced Scorecard to improve the pharmacy's performance.

5.2 COSO ERM Applications

The effect of applying the COSO-ERM model in commercial banks was tested by Rahman & Al-Dhaimesh (2018). Furthermore, the study identified the role of each board of directors, audit committee, executive management, human resource management, and internal audit as corporate governance mechanisms in enhancing the effectiveness of internal control systems. The study that was carried out by questionnaires to stakeholders in all commercial banks in Jordan and statistical analysis, revealed a positive 77.8% impact of framework application on preventing fraudulent financial reporting. Moreover, it observed that each of internal control, event identification, risk assessment and response, and control activities variables affect fraudulent financial reporting in commercial banks. Similar results were obtained by a study of Wahyuani (2021) addressing the effect of COSO ERM Framework approach in strategic planning for Islamic banking use. Risk Management has a dual role in achieving corporate strategy, which is as the basic foundation in strategic planning as well as the protection during the implementation of the company's competitive strategy The field application uses quantitative analysis methods with purposive sampling techniques on employees of an Islamic Bank in Indonesia. The results show that the ERM variable has a positive effect on strategy planning of the bank at the level of 72.5%.

As a general remark, we must underline the significant attention given by researchers applying COSO ERM to the importance of internal control functions or systems.

Shayb (2021) based on the theoretical model COSO ERM, developed a tool that companies can use to correctly identify the risks they were exposed to, to prevent operational crises and applied it in a company of automotive industry, which is providing services in the fields of: Rent a car, Operational leasing and Automotive second-hand cars sales. The study used the 2004 COSO cubes logic.

Padro (2015) discusses the applicability of ISO 31000 and COSO ERM in higher education quality assurance framework, concluding that they are quite similar and both fit to be embedded in a Higher Education Governance model.

A roadmap for application of COSO ERM in Oil and Gas industry is examined by Pham (2018). Petroleum companies are capital-intensive and face many risks ranging from exploration, extraction, distribution, volatile commodity prices and the perplexing political landscape. Also, they are in the forefront to adopt many technologies such as robotics, digitization, and IoT. As a conclusion the researcher states that beyond traditional operational safety considerations to implement a secure, vigilant, and resilient program is not only essential for enhancing an oil and gas company's ability to protect operational integrity amid a growing range of cyber threats, but also to achieve operational excellence.

COSO themselves in cooperation with Deloitte have issued a guide for all types of enterprises on how to manage Artificial Intelligence risks by using the ERM framework (COSO & Deloitte, 2021). There is a broad spectrum of AI-related risks like a) bias and reliability issues due to inappropriate or non-representative data, b) inappropriate use of data, c) inability to understand or explain AI model outputs etc. Potential consequences from these risks can include reputational damage, destruction of shareholder value, regulatory fines, and lawsuits, therefore many enterprises slow down the adoption of related technologies. By leveraging the COSO ERM Framework along with the Deloitte's Trustworthy AI framework, organizations can establish an optimum AI program by implementing the following 5 steps: 1) Establish governance structure for AI program, 2) draft an organization-wide strategy to manage the strategic, technical, regulatory, and operational risks of AI, 3) Assess the risks of each AI model used, 4) Develop a portfolio view of risks and opportunities for AI initiatives, 5) formulate an approach to manage AI risks and report to stakeholders for transparency.

5.3 Conclusions derived from literature review

For the literature review above, that although comprehensive, it may be considered far from complete and detailed, the following conclusions can be derived:

- ISO 31000:2018 and COSO ERM are two widely used risk management frameworks in various organizations.
- The majority of applications are in the Banking & Finance sector, but several applications are in other business areas, as well as in public administration entities.
- Drivers for the application of one of the 2 frameworks are mainly:
    - More effective management of risks, by the implementation of risk treatment plans and the monitoring of the progress of risk mitigation activities.

- Improved risk identification and assessment: The implementation of either ISO 31000 or COSO ERM has helped organizations to identify and assess risks in a more comprehensive and systematic way, leading to better decision-making.
- Better alignment of the organization's risk management activities with its strategic objectives.

In all the referred applications it is either explicitly stated or implied that they resulted in increased stakeholders' confidence by demonstrating a structured and disciplined approach to risk management.

In several applications also, there was successful integration of the new framework with other existing management systems, such as quality management, environmental management, and information security management, leading to a more holistic approach to risk management.

Nevertheless, the implementation of these frameworks can be challenging, particularly in organizations with complex structures or cultures that are resistant to change. Effective communication and training are essential to ensure successful implementation.

Overall, the scientific literature suggests that ISO 31000:2018 and COSO ERM are effective risk management frameworks that can provide significant benefits to organizations that implement them. However, successful implementation requires commitment, resources, and effective communication and training.

CHAPTER 6. FIELD DATA OF APPLICATIONS. PREVALENCE AND ADEQUACY FOR BUSINESS

In the context of this thesis and in order to examine whether any of the two standards prevails and whether there are any patterns of applications in businesses worldwide, we carried out a statistical analysis on a sample of companies that apply any of the two or both ISO 31000 and COSO ERM Framework.

For example, in Literature Review we concluded that the industry that mostly applies standardized risk frameworks is the Banking and Finance sector. Is this a conclusion that can be statistically verified?

Also in chapter 4, one of the differences between ISO31000 and COSO ERM is basically the background of the Organization behind each one. ISO is an international organization while the Treadway Commission, although respected all over the globe, remains purely American. Does this mean that COSO ERM is only popular in U.S. enterprises, while ISO 31000 prevails in the rest of the world?

Moreover, does the fact that COSO ERM is more extensive and detailed (see Chapter 4), while ISO 31000 is just about 16 pages, has an impact on the popularity of the standards?

These initial questions drove my effort to identify a bulk of applications worldwide and statistically investigate the statistical significance of criteria like country, economic sector or size of the company in the choice of the most suitable of the two standards.

The research questions and the sample of the research are detailed in the following paragraphs.

I should underline at this point that as both ISO31000 and COSO ERM are guidelines and are not certifiable (see paragraph 4.1) there are not official registry databases of entities that apply them. Therefore, the search of organizations and enterprises that have endorsed any (or both) of the two standards is rather hectic, based mostly on unofficial declarations or statements, as well as on intensive search engines' use and conclusively, prone to challenges and susceptibility. Details about the way I conducted the research and the respective methodology followed are given in paragraph 6.3 below.

6.1 Research Questions

The research questions, of the study are the following:

1. Is any of the two standards prevailing in terms of adoption from enterprises worldwide, in terms of statistical evidence?
    a. Does any of the two prevail in specific countries or continents around the globe and can this be statistically justified?
2. Are there empirical evidence that there is a preference of one of the two standards in relation to the economic sector of the company?
3. Are there any statistical patterns of application of a specific choice, according to the size of the company?

6.2 Research methodology

The research is based on information collected through extensive internet search with keywords like “ISO31000”, “COSO ERM”, “Risk Management Standard” followed by the word “adoption” or “application” or “discussion” in Google and other search engines, as well as scientific databases as Scope, ResearchGate, RePEc, and Google Scholar. The search results included official websites of companies, annual financial or management reports, press releases, articles, references in social media like LinkedIn. On a second stage, the official websites of the companies/entities were visited to collect additional information on the specifics of the organizations like economy sector, assets, country of origin/headquarters. In several cases this additional information was derived from internet sites (mostly economic) that had respective references or mentions and their validity was confirmed as much as possible.

A problem encountered in the research is the fact that neither ISO 31000, nor COSO ERM are officially certified, so as register databases of certified organizations to exist.

While other ISO standards are certifiable, there is no official process to certify application of ISO 31000[8]. Some organizations do provide ISO 31000 training and

[8] https://www.iso.org/iso-31000-risk-management.html/ (last visit 3/3/2023

certification to individuals however, they claim accreditation under ISO 17024 "Conformity assessment - General requirements for bodies operating certification of persons"[9].

The situation is similar with COSO ERM. Organizations can implement the COSO ERM Framework by following the principles and guidelines provided in the framework. However, there is no formal certification process for the COSO ERM Framework for companies either. Since 2018, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides a learning program toward earning the COSO Enterprise Risk Management (ERM) Certificate only for professionals, consultants and board members who provide oversight of ERM[10].

That being clarified, a second problem arises that has to do with the validity of a claim that an entity applies or endorses one or the other standard. Since there is no official auditing process, there is no objective way for the researcher to rely on the research findings. Announcements or press releases that refer to the application of the standards may be just publicity/marketing material. Nevertheless, since the objective of the study is to investigate the prevalence and adequacy of the two standards for businesses, this problem can be overlooked in the present study and mostly eliminated (in the statistical sense) through the size of the sample to be examined.

6.3 The Sample

The final sample exists of 367 entities (companies and state agencies) worldwide.

For those entities, the following information were collected:

- Country of Origin (or of central Headquarters)
  - 43 different countries were recognized.

[9] https://learn31000.com/is-iso-31000-certifiable. (last visit 3/3/2023)

[10] https://www.theiia.org/en/products/learning-solutions/course/coso-enterprise-risk-management-certificate/ . (last visit 3/3/2023)

- Continent of the Country
    - Europe, Asia, Australia, North & South America and Africa.
- Economic Sector of main operations
    - 35 different economic sectors were identified.
- Total Assets (in billion €)
    - This variable has the purpose to show the size of the entity.
    - Total Assets were collected from most recent available information, and may be from the years 2019 to 2021 (the majority). There was no exclusion of any entity if 2021 data could not be found.
    - If expressed in other currency that Euro, the conversion was based on the exchange rate on the last day of the respective year.
- Assets class
    - A discrete variable that takes 8 different values, according to the Total Assets of the entity, as follows:

        0: Total assets not found or the entity is a state fund/organization
        1: Total Assets: 0.1-9.9 bn€
        2: " " : 10-19.9 bn€
        3: " " : 20-49.9 bn€
        4: " " : 50-99.9 bn€
        5: " " : 100-299.9 bn€
        6: " " : 300-999.9 bn€
        7: " " : > 1000 bn€

- Standard

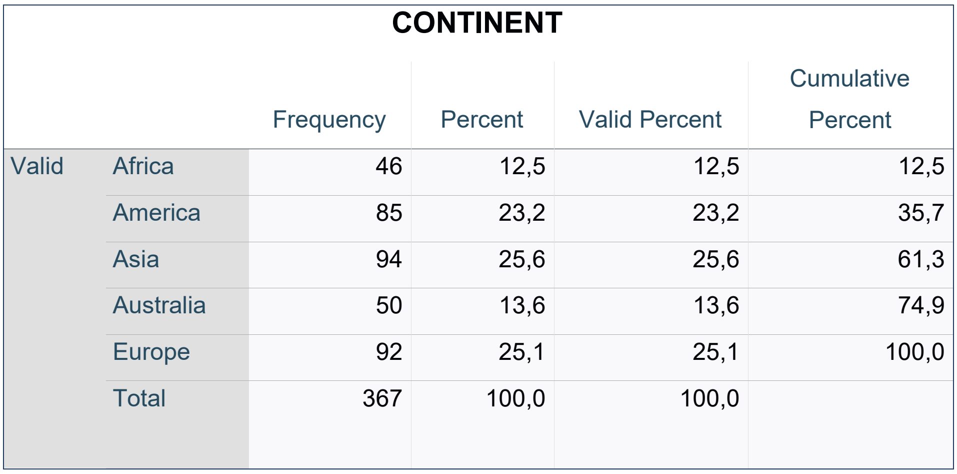
- A variable about the risk standard that the entity follows, having 3 discrete values:
    - ISO 31000
    - COSO ERM
    - Both

6.3.1 Descriptive Statistics of the sample

In this section, the sample data are analyzed per criterion, a table with frequencies and percentages is presented, as well as a suitable diagram for visualizing the outcomes.

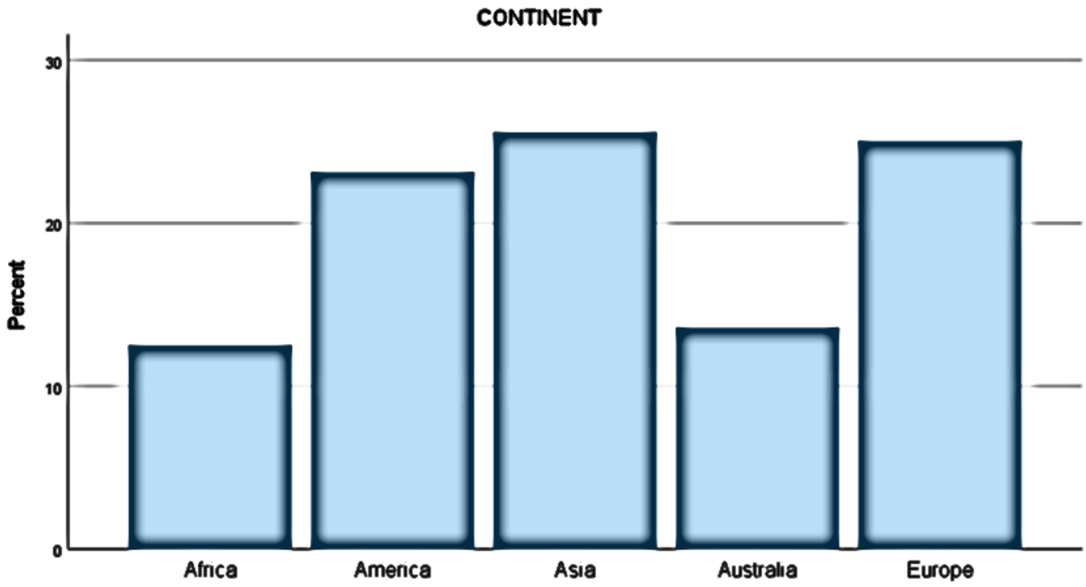
a) Continent

Although the list of entities is far from being exhaustive in order to derive more accurate conclusions, the majority of entities are Asian or European (25.6% and 25.1%, respectively), followed by American (23.2%).



CONTINENT

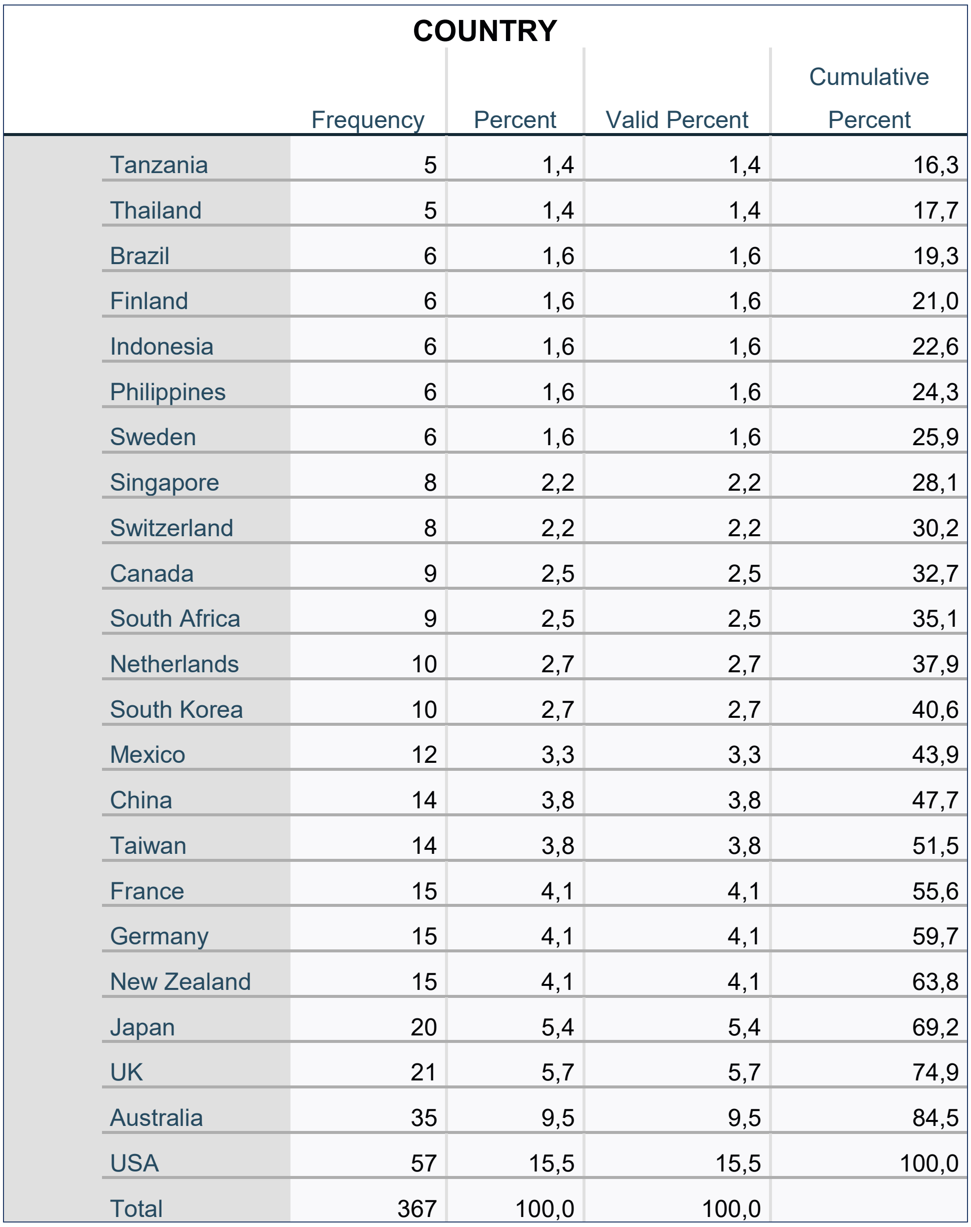
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Africa	46	12,5	12,5	12,5
	America	85	23,2	23,2	35,7
	Asia	94	25,6	25,6	61,3
	Australia	50	13,6	13,6	74,9
	Europe	92	25,1	25,1	100,0
	Total	367	100,0	100,0	



b) Country

COUNTRY

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Algeria	1	,3	,3	,3
	Chile	1	,3	,3	,5
	Denmark	1	,3	,3	,8
	Saudi Arabia	1	,3	,3	1,1
	Togo	1	,3	,3	1,4
	Cote d'Ivoire	2	,5	,5	1,9
	India	2	,5	,5	2,5
	Tunisia	2	,5	,5	3,0
	Uganda	2	,5	,5	3,5
	Rwanda	3	,8	,8	4,4
	Senegal	3	,8	,8	5,2
	Egypt	4	1,1	1,1	6,3
	Hong Kong	4	1,1	1,1	7,4
	Malaysia	4	1,1	1,1	8,4
	Morocco	4	1,1	1,1	9,5
	Italy	5	1,4	1,4	10,9
	Kenya	5	1,4	1,4	12,3
	Nigeria	5	1,4	1,4	13,6
	Spain	5	1,4	1,4	15,0

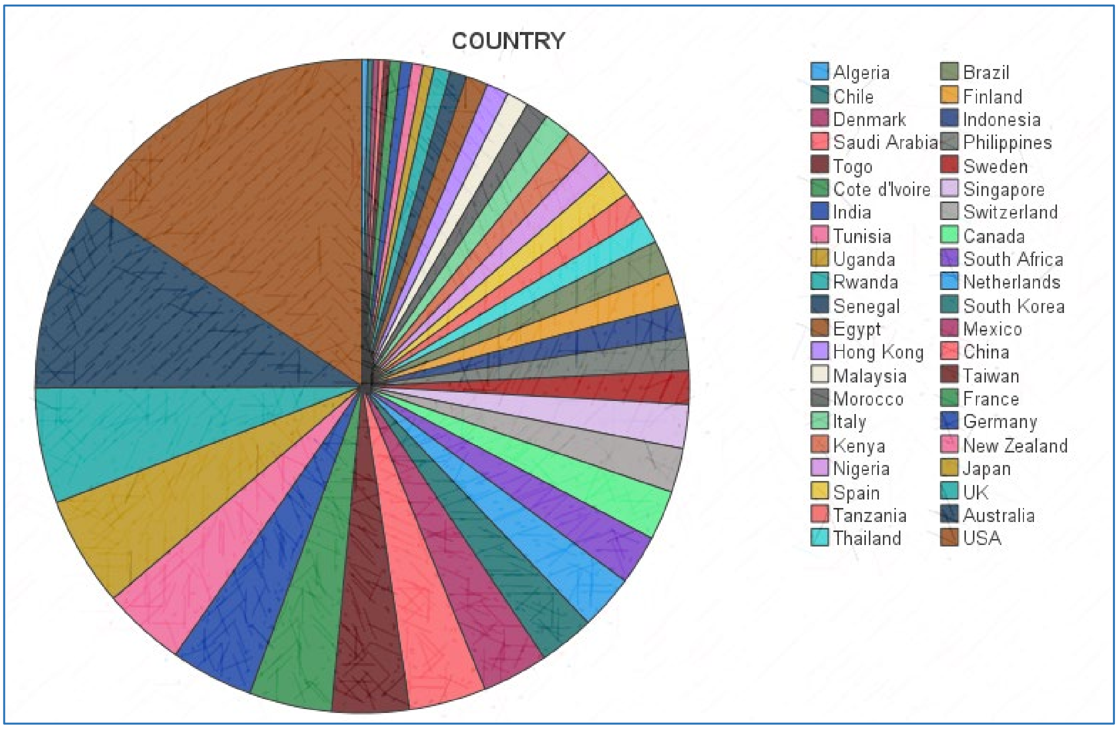


COUNTRY

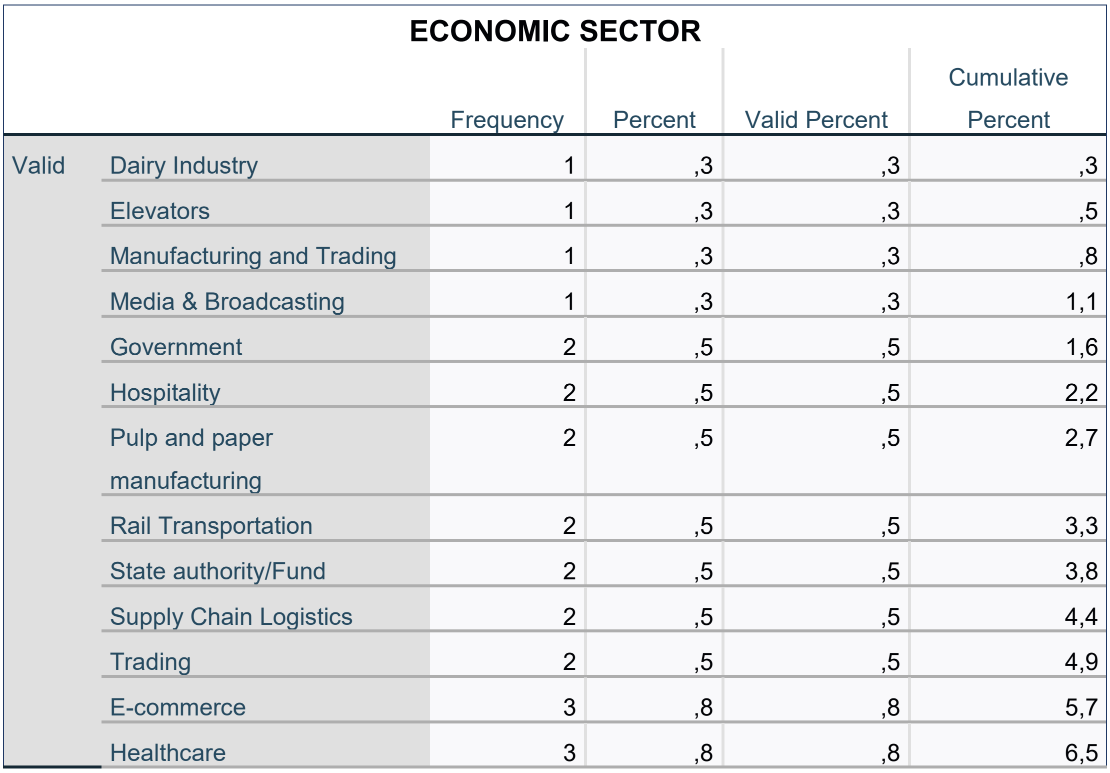
	Frequency	Percent	Valid Percent	Cumulative Percent
Tanzania	5	1,4	1,4	16,3
Thailand	5	1,4	1,4	17,7
Brazil	6	1,6	1,6	19,3
Finland	6	1,6	1,6	21,0
Indonesia	6	1,6	1,6	22,6
Philippines	6	1,6	1,6	24,3
Sweden	6	1,6	1,6	25,9
Singapore	8	2,2	2,2	28,1
Switzerland	8	2,2	2,2	30,2
Canada	9	2,5	2,5	32,7
South Africa	9	2,5	2,5	35,1
Netherlands	10	2,7	2,7	37,9
South Korea	10	2,7	2,7	40,6
Mexico	12	3,3	3,3	43,9
China	14	3,8	3,8	47,7
Taiwan	14	3,8	3,8	51,5
France	15	4,1	4,1	55,6
Germany	15	4,1	4,1	59,7
New Zealand	15	4,1	4,1	63,8
Japan	20	5,4	5,4	69,2
UK	21	5,7	5,7	74,9
Australia	35	9,5	9,5	84,5
USA	57	15,5	15,5	100,0
Total	367	100,0	100,0	

The total sample consists of 42 countries.

15.5% of the sample entities are from USA and an additional 13.6% from Australia and New Zealand. These 3 countries with UK, Japan, Germany and France constitute 44.4% of the total sample, followed by China and Taiwan (an additional 7.1%).



c) Economic Sector



ECONOMIC SECTOR

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Dairy Industry	1	,3	,3	,3
	Elevators	1	,3	,3	,5
	Manufacturing and Trading	1	,3	,3	,8
	Media & Broadcasting	1	,3	,3	1,1
	Government	2	,5	,5	1,6
	Hospitality	2	,5	,5	2,2
	Pulp and paper manufacturing	2	,5	,5	2,7
	Rail Transportation	2	,5	,5	3,3
	State authority/Fund	2	,5	,5	3,8
	Supply Chain Logistics	2	,5	,5	4,4
	Trading	2	,5	,5	4,9
	E-commerce	3	,8	,8	5,7
	Healthcare	3	,8	,8	6,5

ECONOMIC SECTOR

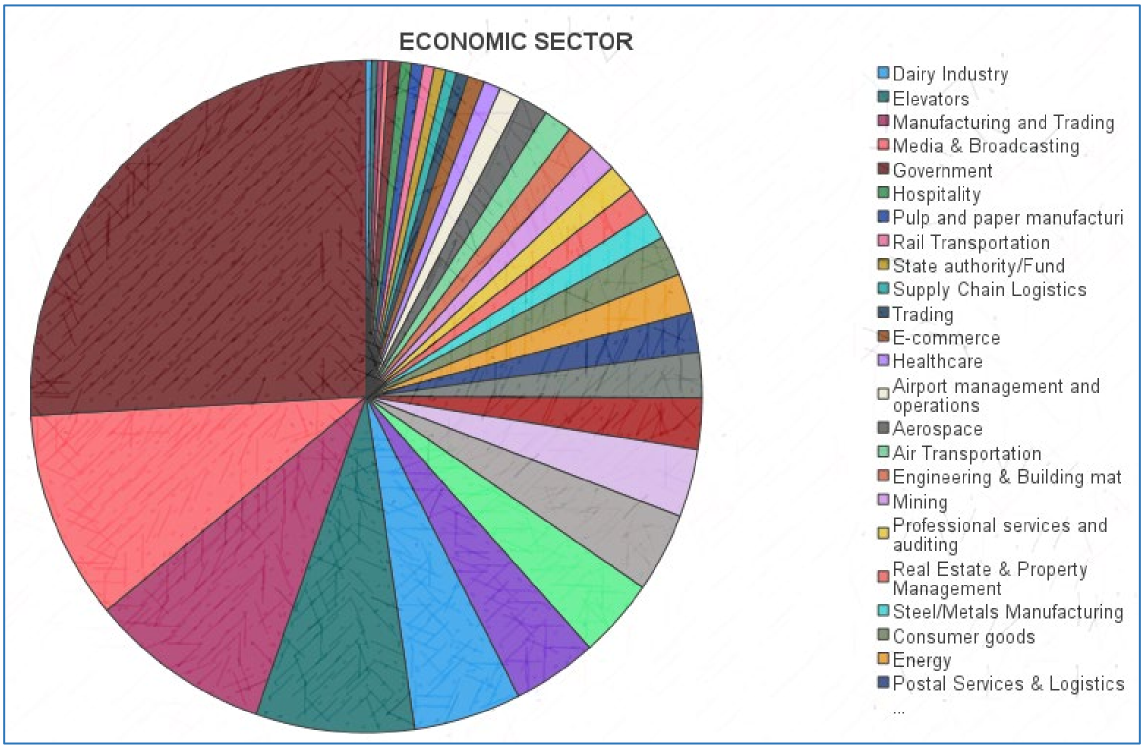
	Frequency	Percent	Valid Percent	Cumulative Percent
Airport management and operations	4	1,1	1,1	7,6
Aerospace	5	1,4	1,4	9,0
Air Transportation	5	1,4	1,4	10,4
Engineering & Building materials	5	1,4	1,4	11,7
Mining	5	1,4	1,4	13,1
Professional services and auditing	5	1,4	1,4	14,4
Real Estate & Property Management	5	1,4	1,4	15,8
Steel/Metals Manufacturing	5	1,4	1,4	17,2
Consumer goods	7	1,9	1,9	19,1
Energy	7	1,9	1,9	21,0
Postal Services & Logistics	7	1,9	1,9	22,9
Retail	8	2,2	2,2	25,1
Chemicals	9	2,5	2,5	27,5
Pharmaceuticals	12	3,3	3,3	30,8
Automotive industry	14	3,8	3,8	34,6
Insurance	14	3,8	3,8	38,4
Electric Utility	15	4,1	4,1	42,5
Food & beverage	19	5,2	5,2	47,7
Oil and Gas Exploration and Production	28	7,6	7,6	55,3
Technology/Electronics	32	8,7	8,7	64,0
Telecommunications	37	10,1	10,1	74,1
Banking and Financial Services	95	25,9	25,9	100,0
Total	367	100,0	100,0	

Economic activity was separated in 35 sectors.

The vast majority of the sample comes from the “Banking and Financial Services” sector (25.9%), leading to the conclusion that this business area is more risk avert and more eager than others to apply risk management measures in daily operations. The second higher percentage comes from the “Telecommunications” sector (10.1%).

These 2 sectors with the addition of “Technology/Electronics” and “Oil & Gas Exploration & Production” make up the 52.3% of the total sample.

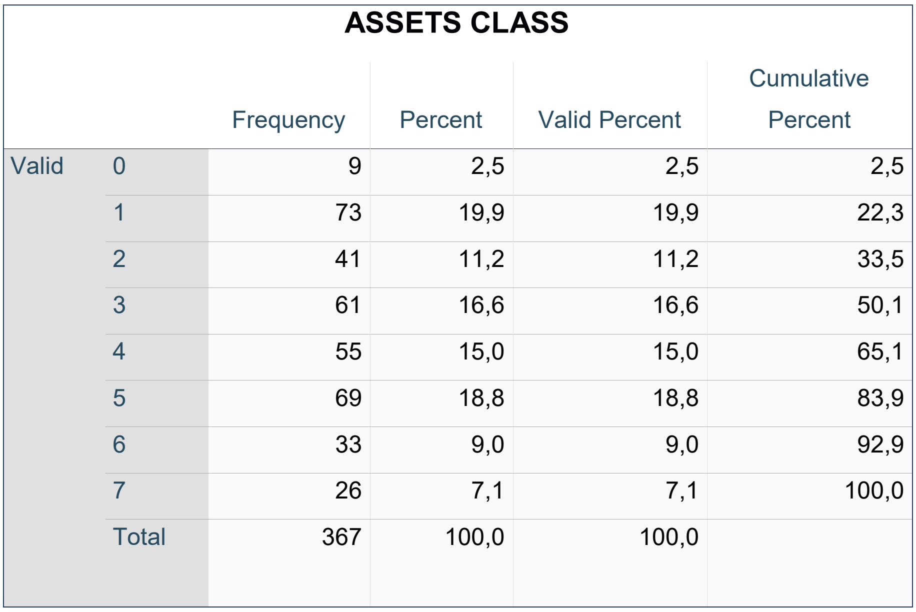
Two states (Australia and Canada) apply ISO 31000 to all their official governmental activities, while additional 2 commonwealth funds of the Australian state comply with both standards.



d) Assets’ Class

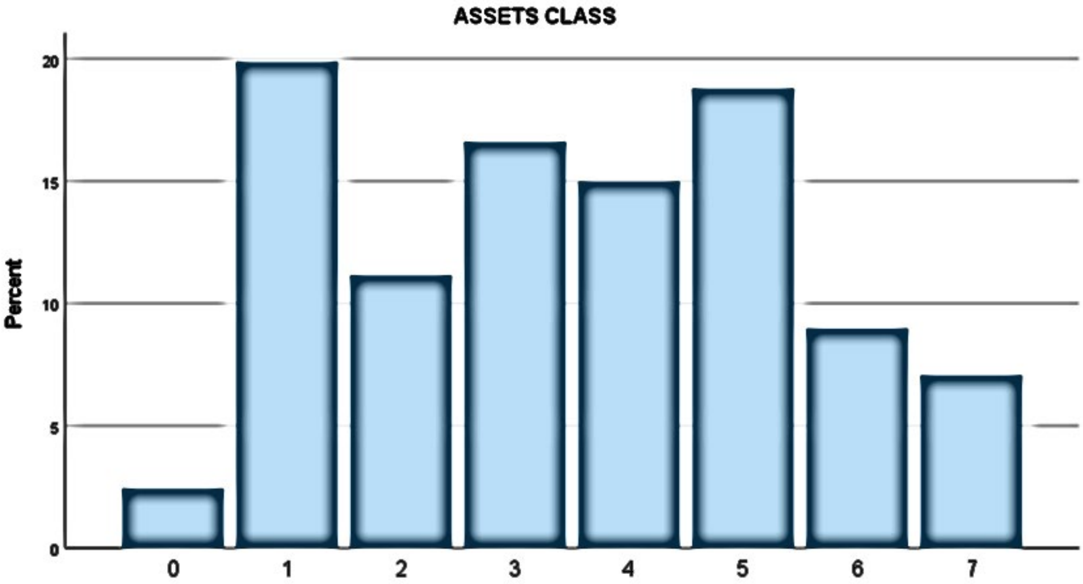
For 9 entities (2.5%) the Assets’ Class variable has N/A value, either because it refers to governmental and state entities (4 cases), or the respective information could not be found.

Apart from the above, the rest of the sample is quite balanced including companies from all the classes.



ASSETS CLASS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	9	2,5	2,5	2,5
	1	73	19,9	19,9	22,3
	2	41	11,2	11,2	33,5
	3	61	16,6	16,6	50,1
	4	55	15,0	15,0	65,1
	5	69	18,8	18,8	83,9
	6	33	9,0	9,0	92,9
	7	26	7,1	7,1	100,0
	Total	367	100,0	100,0	



0: Total assets N/A
1: Total Assets: 0.1-9.9 bn€
2: “ “ : 10-19.9 bn€
3: “ “ : 20-49.9 bn€
4: “ “ : 50-99.9 bn€
5: “ “ : 100-299.9 bn€
6: “ “ : 300-999.9 bn€
7: “ “ : > 1000 bn€

6.4 Statistical Analysis Method

The statistical package SPSS 28.0.0.0 was used for the statistical analysis of the data.

The Excel file of the sample data, after clean-up, was uploaded to SPSS, where it was converted to .sav format and saved.

The analysis methodology followed the following steps:

1. Frequency analysis of variables & descriptive statistics

2. Pairwise tests of independence of variables and correlations matrix.

The results of the analysis from SPSS were saved in .spv format, "Exported" in .xlsx or docx format, as the case may be, and then copy-pasted into this Word file.

CHAPTER 7. STATISTICAL ANALYSIS AND DISCUSSION OF THE RESULTS

7.1 Theoretic Background

The variables we used in the study are qualitative. Qualitative are the variables whose value is given in words and are divided into 2 types according to the scale they follow:

α) Nominal: relating to physical categories without arrangement (e.g. Country, Continent, Economic Sector)

β) Ordinal: that are also expressed in words, but there is an order between the alternative answers (eg Assets Class).

7.1.1 Independence tests X^2

The non-parametric test X^2 (Pearson's chi-square) is used in samples of qualitative variables, as in our case, to test whether two variables X and Y of a sample are dependent or independent and is called "test of independence" (Halikias, 2022).

The X^2 test is based on the Crosstabulation or contigency table, which is a double input of the two variables, in the cells of which the frequencies per pair of categories of the 2 variables are recorded, and on the X^2 value resulting from it, making the initial assumption:

- H0: the two variables are independent.
- The alternative hypothesis H1: is that the two variables are dependent.

With SPSS we calculate X^2 and its asymptotic significance level. If this is less than 0.05 i.e., 5%, then the hypothesis H0 of independence of the variables must be rejected, meaning that they are dependent/correlated with each other.

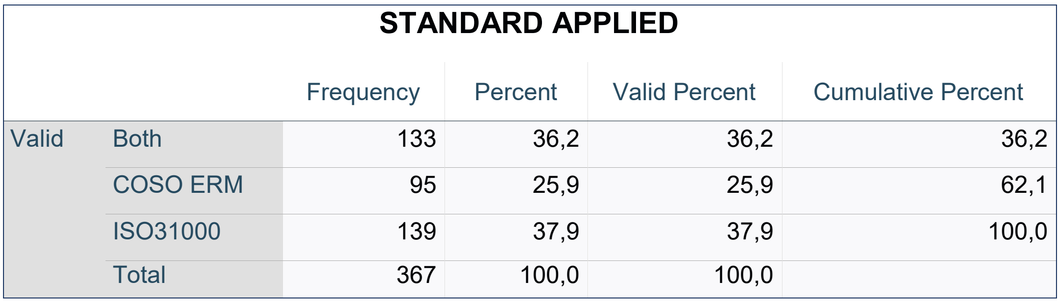
The X^2 test is applied under the conditions that a) the sample size is at least four times the number of cells and b) the expected frequencies are not less than 1 and 25% of them are not less than 5. If these two conditions are not met then in the case of 2 x 2 cells, Fisher's exact statistic is used, while in any other case, neighboring cells must be merged in such a way that the new variable that results has meaning (Tsandas et.al, 1999).

To investigate the intensity and nature of the relationship between the two variables, once the hypothesis of their independence is rejected, a number of statistical measures are available, such as Pearson's Phi coefficient. When we have ordinal qualitative variables, we usually use the Kendal-τ coefficient (Kendal tau) which determines the nature (positive or negative) and the intensity (strong or weak) of the correlation.

The calculation of Pearson's Phi coefficients, Eta and Kendall's tau-b (suitable for symmetric tables) or Kendall's tau-c (suitable for non-symmetric tables) is also done with SPSS (Halikias, 2022).

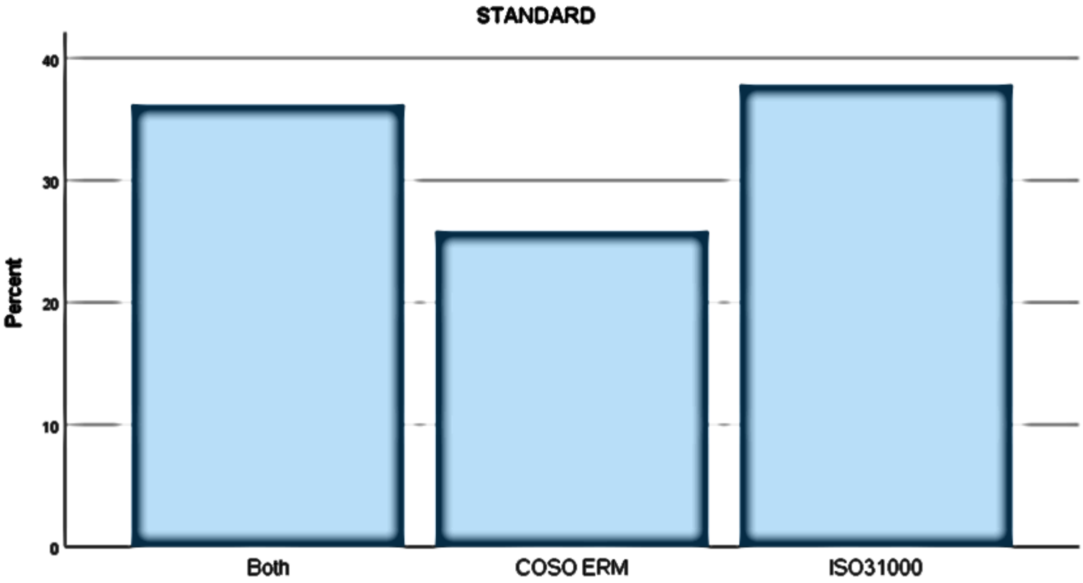
7.2 Statistics about the standard applied in the sample

The majority of entities in the sample (37.9%) apply only ISO 31000, while 25.9% apply only COSO ERM. A big percentage (36.2%) claims to apply both. This finding is consistent with other surveys (see in Chapter 5) that also indicate that ISO is more popular than COSO standard. Moreover, even if it initially seems surprising that a big number of entities applies both, this is logical since it is not very difficult to comply with the second standard if one has already applied the first and this attitude shows also commitment to risk management from the side of the top management of the company.



STANDARD APPLIED

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Both	133	36,2	36,2	36,2
	COSO ERM	95	25,9	25,9	62,1
	ISO31000	139	37,9	37,9	100,0
	Total	367	100,0	100,0	



7.3 Independence Tests and Variable Correlations

In the context of this thesis, we will investigate the existence of a possible correlation between the STANDARD variable and the rest of variables within the sample, conducting respective independence tests X^2.

The results are presented below for each case including:

a) The crosstab,

b) The X^2 tests

c) The Kendall’s tau-c measure of correlation

d) A clustered bar chart to visualize the outcomes and

e) The conclusion(s) and any commentary thereof.

A) CONTINENT * STANDARD Crosstabulation

Crosstab

			STANDARD			
			Both	COSO ERM	ISO31000	Total
CONTINENT	Africa	Count	0	0	46	46
		Expected Count	16,7	11,9	17,4	46,0
		% within CONTINENT	0,0%	0,0%	100,0%	100,0%
	America	Count	41	21	23	85
		Expected Count	30,8	22,0	32,2	85,0
		% within CONTINENT	48,2%	24,7%	27,1%	100,0%
	Asia	Count	10	41	43	94
		Expected Count	34,1	24,3	35,6	94,0
		% within CONTINENT	10,6%	43,6%	45,7%	100,0%
	Australia	Count	49	0	1	50
		Expected Count	18,1	12,9	18,9	50,0
		% within CONTINENT	98,0%	0,0%	2,0%	100,0%
	Europe	Count	33	33	26	92
		Expected Count	33,3	23,8	34,8	92,0
		% within CONTINENT	35,9%	35,9%	28,3%	100,0%
Total		Count	133	95	139	367
		Expected Count	133,0	95,0	139,0	367,0
		% within CONTINENT	36,2%	25,9%	37,9%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	199,805[a]	8	<,001
Likelihood Ratio	227,083	8	<,001
N of Valid Cases	367		

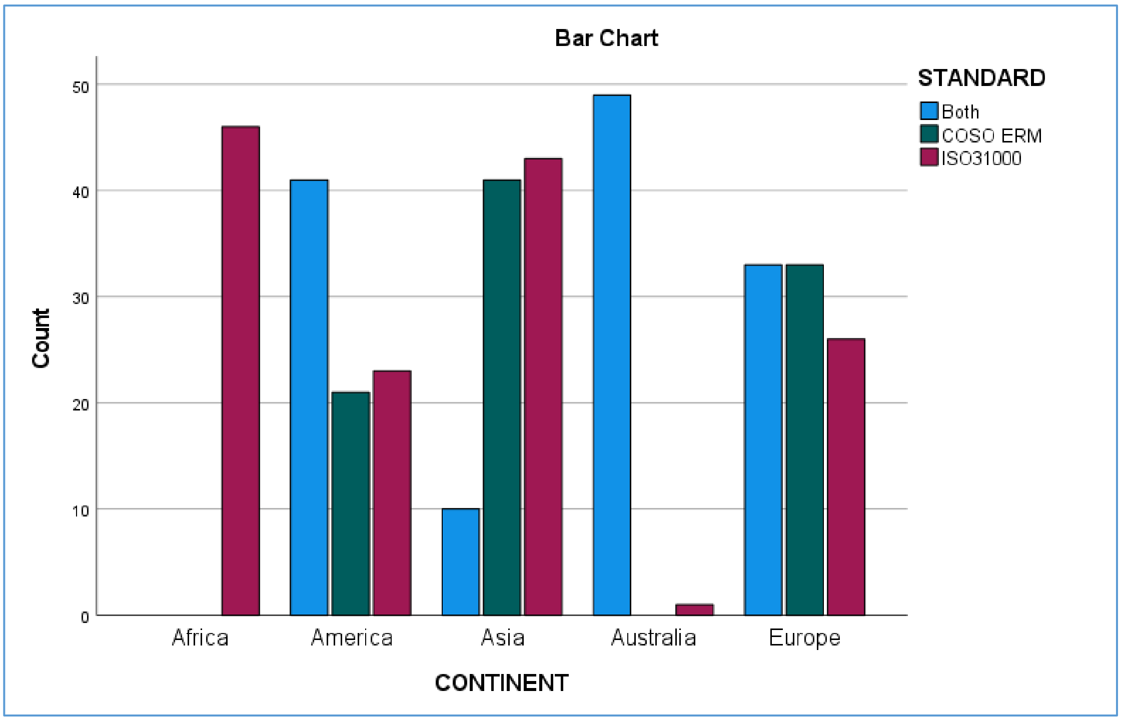
a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 11,91.

Symmetric Measures

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Ordinal by Ordinal	Kendall's tau-c	-,282	,047	-5,934	<,001
N of Valid Cases		367			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.



In the test of independence of the CONTINENT and STANDARD variables, we first see the Crosstab where the rows refer to the values of CONTINENT variable and the columns to the values of STANDARD variable. In each cell they are calculated:

a. the number of observations (count)

b. the expected value of the observations, based on the sample, which should not differ much from the number of observations, in case of independence of variables.

c. the percentage of observations for each value of the STANDARD variable

In the case of AFRICA, for example, we see that all companies observed apply solely the ISO 31000.

In the case of AMERICA, COSO applications are nearly as many as expected (count=21, expected=22), yet more than expected companies apply BOTH standards and statistically less prefer the ISO 31000.

ASIAN companies prefer to a large extend solely one of the two standards, while 98% of AUSTRALIAN entities apply BOTH standards.

Finally, in EUROPE the situation is rather mixed with almost equal application of either one of the two or both standards.

These initial conclusions are confirmed in the Chi-Square Tests Table, where X^2 is calculated and which has an asymptotic significance level of $p<0.05$, which proves that we have to reject the hypothesis of independence of the 2 variables.

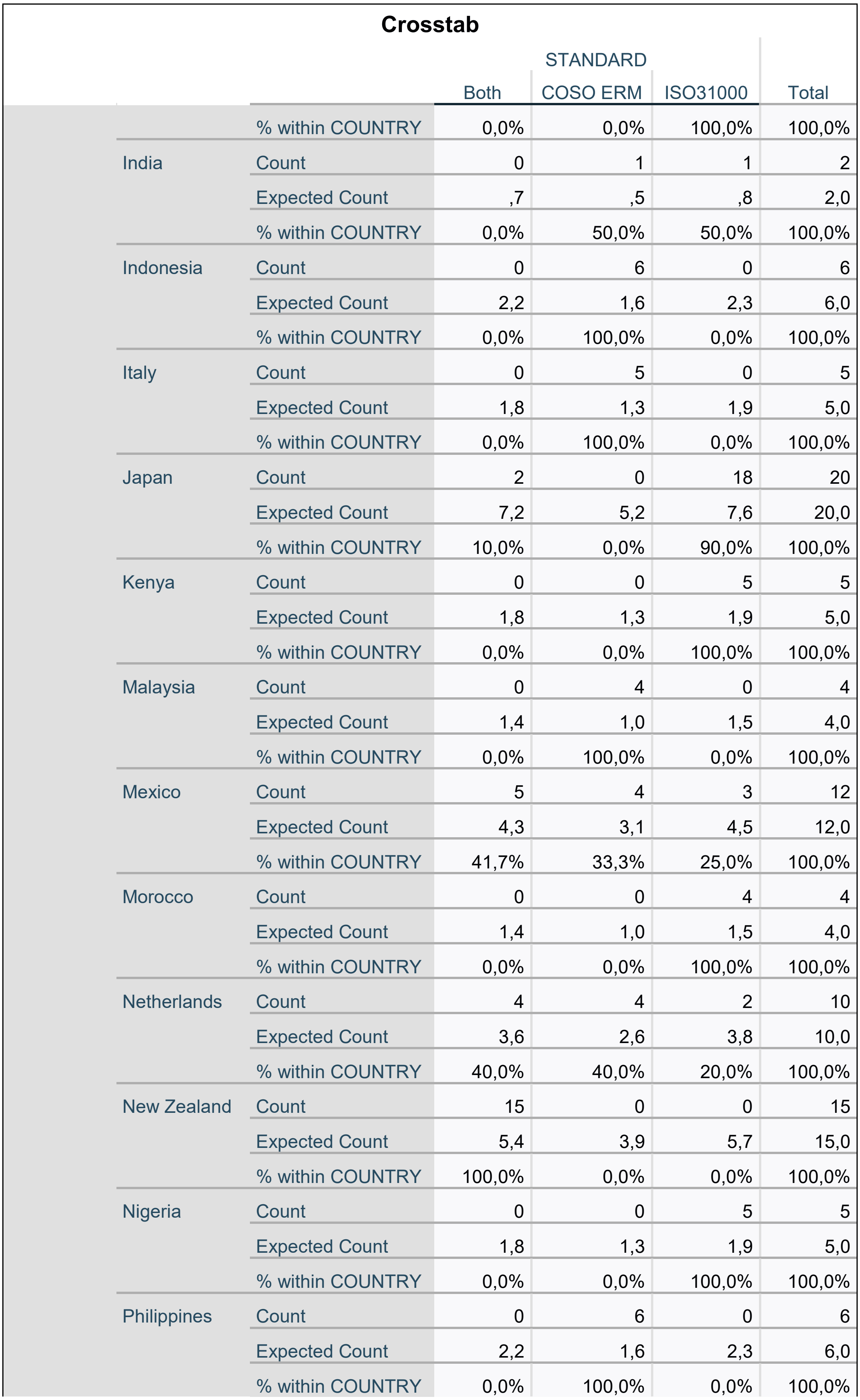
The next Symmetric Measures table calculates the Kendall's tau parameter and we see that it has a Kendall's tau-c value (suitable for non-symmetric tables) $\tau= -0.282 <0.3$ which means there is a weak negative correlation between the 2 variables. This can be interpreted in a manner of “as CONTINENT variable moves from AFRICA to EUROPE, the STANDARD variable moves (weakly) in the opposite direction, i.e., from ISO to BOTH”

All the above are visualized in the corresponding bar graph.

B) COUNTRY * STANDARD Crosstabulation

Crosstab

			STANDARD			
			Both	COSO ERM	ISO31000	Total
COUNTRY	Algeria	Count	0	0	1	1
		Expected Count	,4	,3	,4	1,0
		% within COUNTRY	0,0%	0,0%	100,0%	100,0%
	Australia	Count	34	0	1	35
		Expected Count	12,7	9,1	13,3	35,0
		% within COUNTRY	97,1%	0,0%	2,9%	100,0%
	Brazil	Count	2	0	4	6
		Expected Count	2,2	1,6	2,3	6,0
		% within COUNTRY	33,3%	0,0%	66,7%	100,0%
	Canada	Count	1	7	1	9
		Expected Count	3,3	2,3	3,4	9,0
		% within COUNTRY	11,1%	77,8%	11,1%	100,0%
	China	Count	0	8	6	14
		Expected Count	5,1	3,6	5,3	14,0
		% within COUNTRY	0,0%	57,1%	42,9%	100,0%
	Cote d'Ivoire	Count	0	0	2	2
		Expected Count	,7	,5	,8	2,0
		% within COUNTRY	0,0%	0,0%	100,0%	100,0%
	Denmark	Count	1	0	0	1
		Expected Count	,4	,3	,4	1,0
		% within COUNTRY	100,0%	0,0%	0,0%	100,0%
	Egypt	Count	0	0	4	4
		Expected Count	1,4	1,0	1,5	4,0
		% within COUNTRY	0,0%	0,0%	100,0%	100,0%
	Finland	Count	2	2	2	6
		Expected Count	2,2	1,6	2,3	6,0
		% within COUNTRY	33,3%	33,3%	33,3%	100,0%
	France	Count	5	4	6	15
		Expected Count	5,4	3,9	5,7	15,0
		% within COUNTRY	33,3%	26,7%	40,0%	100,0%
	Germany	Count	7	7	1	15
		Expected Count	5,4	3,9	5,7	15,0
		% within COUNTRY	46,7%	46,7%	6,7%	100,0%
	Hong Kong	Count	0	0	4	4
		Expected Count	1,4	1,0	1,5	4,0



Crosstab

		STANDARD			
		Both	COSO ERM	ISO31000	Total
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
India	Count	0	1	1	2
	Expected Count	,7	,5	,8	2,0
	% within COUNTRY	0,0%	50,0%	50,0%	100,0%
Indonesia	Count	0	6	0	6
	Expected Count	2,2	1,6	2,3	6,0
	% within COUNTRY	0,0%	100,0%	0,0%	100,0%
Italy	Count	0	5	0	5
	Expected Count	1,8	1,3	1,9	5,0
	% within COUNTRY	0,0%	100,0%	0,0%	100,0%
Japan	Count	2	0	18	20
	Expected Count	7,2	5,2	7,6	20,0
	% within COUNTRY	10,0%	0,0%	90,0%	100,0%
Kenya	Count	0	0	5	5
	Expected Count	1,8	1,3	1,9	5,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Malaysia	Count	0	4	0	4
	Expected Count	1,4	1,0	1,5	4,0
	% within COUNTRY	0,0%	100,0%	0,0%	100,0%
Mexico	Count	5	4	3	12
	Expected Count	4,3	3,1	4,5	12,0
	% within COUNTRY	41,7%	33,3%	25,0%	100,0%
Morocco	Count	0	0	4	4
	Expected Count	1,4	1,0	1,5	4,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Netherlands	Count	4	4	2	10
	Expected Count	3,6	2,6	3,8	10,0
	% within COUNTRY	40,0%	40,0%	20,0%	100,0%
New Zealand	Count	15	0	0	15
	Expected Count	5,4	3,9	5,7	15,0
	% within COUNTRY	100,0%	0,0%	0,0%	100,0%
Nigeria	Count	0	0	5	5
	Expected Count	1,8	1,3	1,9	5,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Philippines	Count	0	6	0	6
	Expected Count	2,2	1,6	2,3	6,0
	% within COUNTRY	0,0%	100,0%	0,0%	100,0%

Crosstab

		STANDARD			
		Both	COSO ERM	ISO31000	Total
Rwanda	Count	0	0	3	3
	Expected Count	1,1	,8	1,1	3,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Saudi Arabia	Count	0	0	1	1
	Expected Count	,4	,3	,4	1,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Senegal	Count	0	0	3	3
	Expected Count	1,1	,8	1,1	3,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Singapore	Count	0	0	8	8
	Expected Count	2,9	2,1	3,0	8,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
South Africa	Count	0	0	9	9
	Expected Count	3,3	2,3	3,4	9,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
South Korea	Count	4	2	4	10
	Expected Count	3,6	2,6	3,8	10,0
	% within COUNTRY	40,0%	20,0%	40,0%	100,0%
Spain	Count	0	5	0	5
	Expected Count	1,8	1,3	1,9	5,0
	% within COUNTRY	0,0%	100,0%	0,0%	100,0%
Sweden	Count	1	0	5	6
	Expected Count	2,2	1,6	2,3	6,0
	% within COUNTRY	16,7%	0,0%	83,3%	100,0%
Switzerland	Count	7	1	0	8
	Expected Count	2,9	2,1	3,0	8,0
	% within COUNTRY	87,5%	12,5%	0,0%	100,0%
Taiwan	Count	4	9	1	14
	Expected Count	5,1	3,6	5,3	14,0
	% within COUNTRY	28,6%	64,3%	7,1%	100,0%
Tanzania	Count	0	0	5	5
	Expected Count	1,8	1,3	1,9	5,0
	% within COUNTRY	0,0%	0,0%	100,0%	100,0%
Thailand	Count	0	5	0	5
	Expected Count	1,8	1,3	1,9	5,0
	% within COUNTRY	0,0%	100,0%	0,0%	100,0%
Tunisia	Count	0	0	2	2

Crosstab

			STANDARD			
			Both	COSO ERM	ISO31000	Total
		Expected Count	,7	,5	,8	2,0
		% within COUNTRY	0,0%	0,0%	100,0%	100,0%
	Uganda	Count	0	0	2	2
		Expected Count	,7	,5	,8	2,0
		% within COUNTRY	0,0%	0,0%	100,0%	100,0%
	UK	Count	6	5	10	21
		Expected Count	7,6	5,4	8,0	21,0
		% within COUNTRY	28,6%	23,8%	47,6%	100,0%
	USA	Count	33	10	14	57
		Expected Count	20,7	14,8	21,6	57,0
		% within COUNTRY	57,9%	17,5%	24,6%	100,0%
Total		Count	133	95	139	367
		Expected Count	133,0	95,0	139,0	367,0
		% within COUNTRY	36,2%	25,9%	37,9%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	370,853[a]	82	<,001
Likelihood Ratio	403,100	82	<,001
N of Valid Cases	367		

a. 104 cells (82,5%) have expected count less than 5. The minimum expected count is ,26.

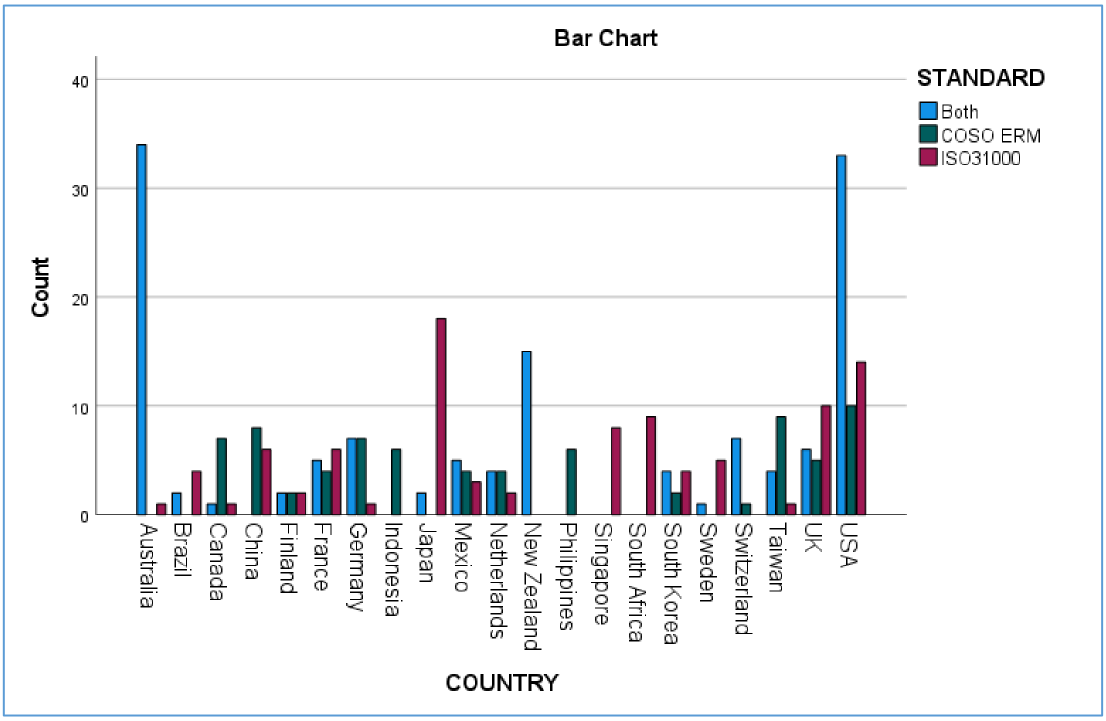
Symmetric Measures[c]

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Ordinal by Ordinal	Kendall's tau-b	,039	,045	,867	,386
N of Valid Cases		367			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Correlation statistics are available for numeric data only.



From the crosstab, we can conclude the following:

- Countries that have a remarkable preference for ISO 31000 are:
    - Japan, Brazil, Singapore, South Africa, Sweden and UK
- Countries that rather prefer COSO ERM are:
    - Canada, China, Germany, Indonesia, Philippines and Taiwan
- Countries that have a remarkable preference for BOTH standards are:
    - Australia, New Zealand, Switzerland and USA

Chi-Square Tests Table, where X^2 is calculated exhibit an asymptotic significance level of $p<0.05$, which leads to the conclusion that we have to reject the hypothesis of independence of the 2 variables.

Yet, from the Symmetric Measures table we see that Kendall's tau-c value (suitable for non-symmetric tables) $\tau = 0.039$ is very small, meaning that the correlation between the 2 variables is in fact very weak.

All the above are visualized in the corresponding bar graph.

C) ECONOMIC SECTOR * STANDARD

Crosstab

			STANDARD			
			Both	COSO ERM	ISO31000	Total
ECONOMIC SECTOR	Aerospace	Count	4	0	1	5
		Expected Count	1,8	1,3	1,9	5,0
		% within ECONOMIC SECTOR	80,0%	0,0%	20,0%	100,0%
	Air Transportation	Count	2	1	2	5
		Expected Count	1,8	1,3	1,9	5,0
		% within ECONOMIC SECTOR	40,0%	20,0%	40,0%	100,0%
	Airport management and operations	Count	2	2	0	4
		Expected Count	1,4	1,0	1,5	4,0
		% within ECONOMIC SECTOR	50,0%	50,0%	0,0%	100,0%
	Automotive industry	Count	6	3	5	14
		Expected Count	5,1	3,6	5,3	14,0
		% within ECONOMIC SECTOR	42,9%	21,4%	35,7%	100,0%
	Banking and Financial Services	Count	28	35	32	95
		Expected Count	34,4	24,6	36,0	95,0
		% within ECONOMIC SECTOR	29,5%	36,8%	33,7%	100,0%
	Chemicals	Count	3	2	4	9
		Expected Count	3,3	2,3	3,4	9,0
		% within ECONOMIC SECTOR	33,3%	22,2%	44,4%	100,0%
	Consumer goods	Count	2	2	3	7
		Expected Count	2,5	1,8	2,7	7,0
		% within ECONOMIC SECTOR	28,6%	28,6%	42,9%	100,0%
	Dairy Industry	Count	1	0	0	1
		Expected Count	,4	,3	,4	1,0
		% within ECONOMIC SECTOR	100,0%	0,0%	0,0%	100,0%
	E-commerce	Count	1	0	2	3
		Expected Count	1,1	,8	1,1	3,0
		% within ECONOMIC SECTOR	33,3%	0,0%	66,7%	100,0%
	Electric Utility	Count	9	0	6	15
		Expected Count	5,4	3,9	5,7	15,0
		% within ECONOMIC SECTOR	60,0%	0,0%	40,0%	100,0%

Crosstab

		STANDARD			
		Both	COSO ERM	ISO31000	Total
Energy	Count	3	3	1	7
	Expected Count	2,5	1,8	2,7	7,0
	% within ECONOMIC SECTOR	42,9%	42,9%	14,3%	100,0%
Engineering & Building materials	Count	2	0	3	5
	Expected Count	1,8	1,3	1,9	5,0
	% within ECONOMIC SECTOR	40,0%	0,0%	60,0%	100,0%
Food & beverage	Count	7	6	6	19
	Expected Count	6,9	4,9	7,2	19,0
	% within ECONOMIC SECTOR	36,8%	31,6%	31,6%	100,0%
Government	Count	0	0	2	2
	Expected Count	,7	,5	,8	2,0
	% within ECONOMIC SECTOR	0,0%	0,0%	100,0%	100,0%
Healthcare	Count	1	1	1	3
	Expected Count	1,1	,8	1,1	3,0
	% within ECONOMIC SECTOR	33,3%	33,3%	33,3%	100,0%
Hospitality	Count	1	0	1	2
	Expected Count	,7	,5	,8	2,0
	% within ECONOMIC SECTOR	50,0%	0,0%	50,0%	100,0%
Insurance	Count	4	8	2	14
	Expected Count	5,1	3,6	5,3	14,0
	% within ECONOMIC SECTOR	28,6%	57,1%	14,3%	100,0%
Mining	Count	1	2	2	5
	Expected Count	1,8	1,3	1,9	5,0
	% within ECONOMIC SECTOR	20,0%	40,0%	40,0%	100,0%
Oil and Gas Exploration and Production	Count	9	8	11	28
	Expected Count	10,1	7,2	10,6	28,0
	% within ECONOMIC SECTOR	32,1%	28,6%	39,3%	100,0%
Pharmaceuticals	Count	8	2	2	12
	Expected Count	4,3	3,1	4,5	12,0
	% within ECONOMIC SECTOR	66,7%	16,7%	16,7%	100,0%
Postal Services & Logistics	Count	5	1	1	7
	Expected Count	2,5	1,8	2,7	7,0
	% within ECONOMIC SECTOR	71,4%	14,3%	14,3%	100,0%
Professional services and auditing	Count	0	1	4	5
	Expected Count	1,8	1,3	1,9	5,0
	% within ECONOMIC SECTOR	0,0%	20,0%	80,0%	100,0%

Crosstab

			STANDARD			
			Both	COSO ERM	ISO31000	Total
	Pulp and paper manufacturing	Count	1	1	0	2
		Expected Count	,7	,5	,8	2,0
		% within ECONOMIC SECTOR	50,0%	50,0%	0,0%	100,0%
	Rail Transportation	Count	2	0	0	2
		Expected Count	,7	,5	,8	2,0
		% within ECONOMIC SECTOR	100,0%	0,0%	0,0%	100,0%
	Real Estate & Property Management	Count	2	0	3	5
		Expected Count	1,8	1,3	1,9	5,0
		% within ECONOMIC SECTOR	40,0%	0,0%	60,0%	100,0%
	Retail	Count	3	2	3	8
		Expected Count	2,9	2,1	3,0	8,0
		% within ECONOMIC SECTOR	37,5%	25,0%	37,5%	100,0%
	State authority/Fund	Count	2	0	0	2
		Expected Count	,7	,5	,8	2,0
		% within ECONOMIC SECTOR	100,0%	0,0%	0,0%	100,0%
	Steel/Metals Manufacturing	Count	2	0	3	5
		Expected Count	1,8	1,3	1,9	5,0
		% within ECONOMIC SECTOR	40,0%	0,0%	60,0%	100,0%
	Supply Chain Logistics	Count	2	0	0	2
		Expected Count	,7	,5	,8	2,0
		% within ECONOMIC SECTOR	100,0%	0,0%	0,0%	100,0%
	Technology/Electronics	Count	11	7	14	32
		Expected Count	11,6	8,3	12,1	32,0
		% within ECONOMIC SECTOR	34,4%	21,9%	43,8%	100,0%
	Telecommunications	Count	8	8	21	37
		Expected Count	13,4	9,6	14,0	37,0
		% within ECONOMIC SECTOR	21,6%	21,6%	56,8%	100,0%
	Trading	Count	0	0	2	2
		Expected Count	,7	,5	,8	2,0
		% within ECONOMIC SECTOR	0,0%	0,0%	100,0%	100,0%
Total		Count	133	95	139	367
		Expected Count	133,0	95,0	139,0	367,0
		% within ECONOMIC SECTOR	36,2%	25,9%	37,9%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	83,554[a]	68	,097
Likelihood Ratio	98,345	68	,009
N of Valid Cases	367		

a. 85 cells (81,0%) have expected count less than 5. The minimum expected count is ,26.

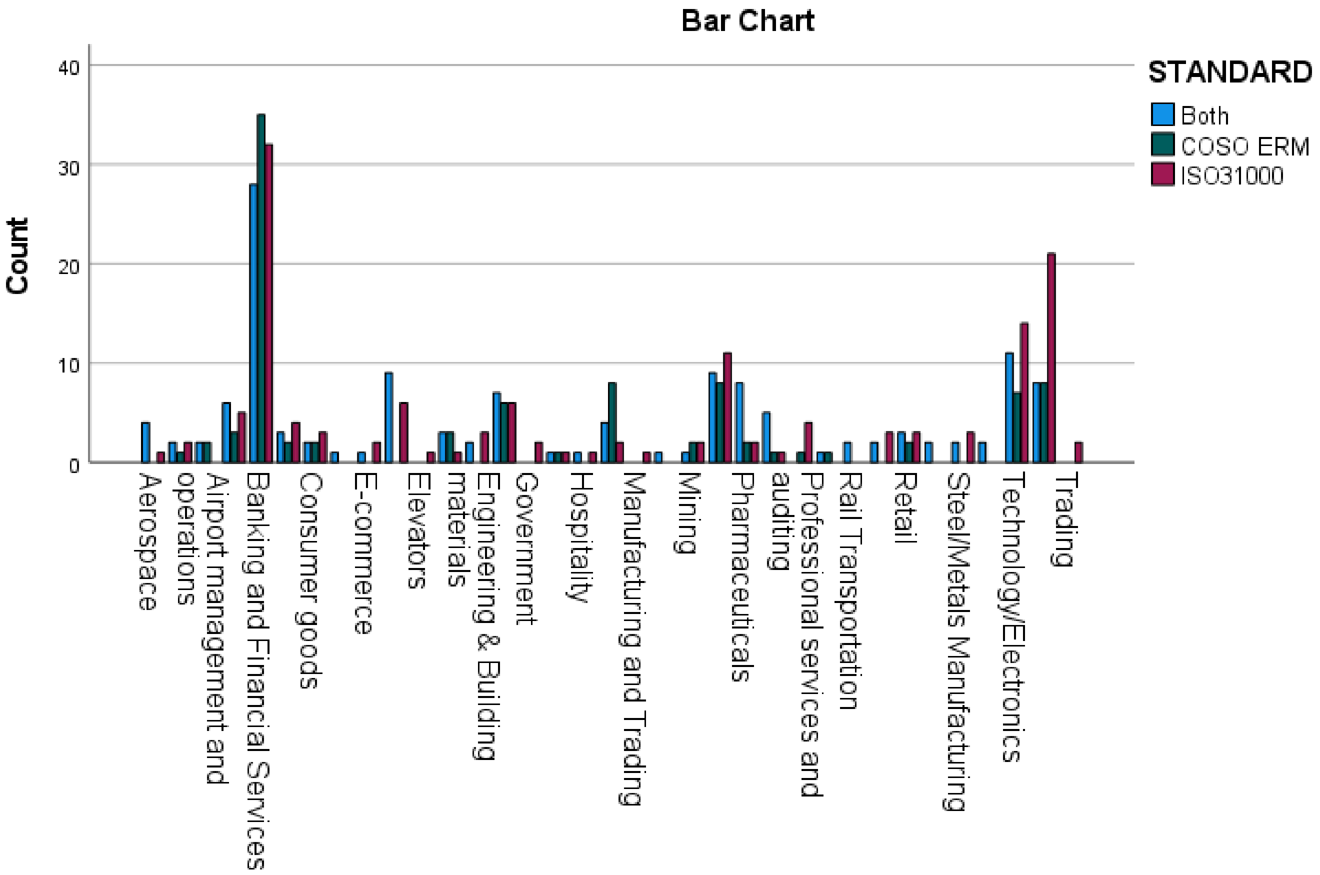
Symmetric Measures[c]

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Ordinal by Ordinal	Kendall's tau-b	,065	,042	1,542	,123
N of Valid Cases		367			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Correlation statistics are available for numeric data only.



From the crosstab, we can conclude the following:

- Sectors that have a remarkable preference for ISO 31000 are:
    - The 2 states (Australia & Canada), Professional services and auditing and Telecommunications
- Sectors that rather prefer COSO ERM are:
    - Banking & Financial Services and Insurance
- Sectors that have a remarkable preference for BOTH standards are:
    - Aerospace industry, Electric utilities, Pharmaceuticals and Postal Services & Logistics
- The rest of economic sectors within the sample do not exhibit any specific trend.

Chi-Square Tests Table, where X^2 is calculated exhibit an asymptotic significance level of $p=0.097>0.05$, which leads to the conclusion that we cannot reject the null hypothesis of independence of the 2 variables.

The above conclusions are visualized in the corresponding bar graph.

D) ASSETS CLASS * STANDARD

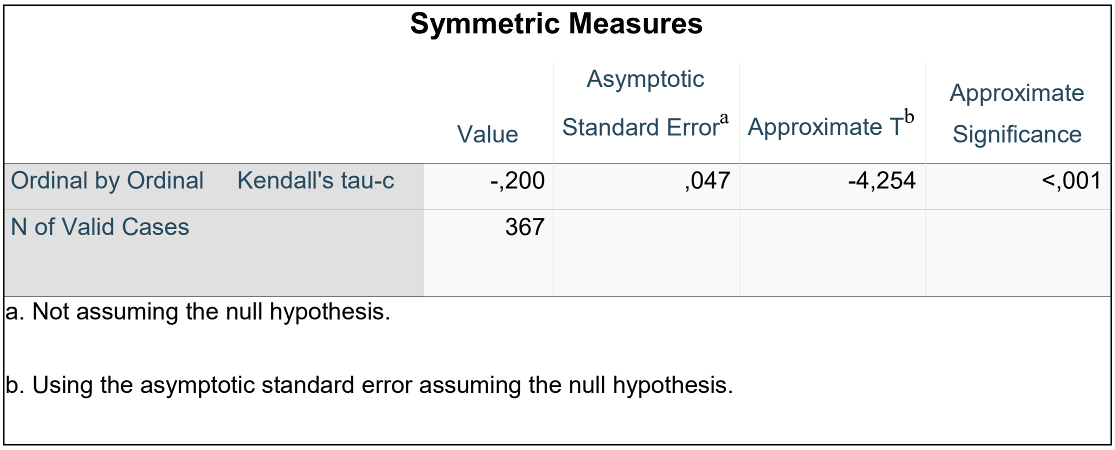
ASSETS CLASS * STANDARD Crosstabulation

			STANDARD			
			Both	COSO ERM	ISO31000	Total
ASSETS CLASS	na	Count	3	2	4	9
		Expected Count	3,3	2,3	3,4	9,0
		% within ASSETS CLASS	33,3%	22,2%	44,4%	100,0%
	0.1-9.9 bn€	Count	25	9	39	73
		Expected Count	26,5	18,9	27,6	73,0
		% within ASSETS CLASS	34,2%	12,3%	53,4%	100,0%
	10-19.9 bn€	Count	13	10	18	41
		Expected Count	14,9	10,6	15,5	41,0
		% within ASSETS CLASS	31,7%	24,4%	43,9%	100,0%
	20-49.9 bn€	Count	14	15	32	61
		Expected Count	22,1	15,8	23,1	61,0
		% within ASSETS CLASS	23,0%	24,6%	52,5%	100,0%
	50-99.9 bn€	Count	21	15	19	55
		Expected Count	19,9	14,2	20,8	55,0
		% within ASSETS CLASS	38,2%	27,3%	34,5%	100,0%
	100-299.9 bn€	Count	30	21	18	69
		Expected Count	25,0	17,9	26,1	69,0
		% within ASSETS CLASS	43,5%	30,4%	26,1%	100,0%
	300-999.9 bn€	Count	14	13	6	33
		Expected Count	12,0	8,5	12,5	33,0
		% within ASSETS CLASS	42,4%	39,4%	18,2%	100,0%
	> 1000 bn€	Count	13	10	3	26
		Expected Count	9,4	6,7	9,8	26,0
		% within ASSETS CLASS	50,0%	38,5%	11,5%	100,0%
Total		Count	133	95	139	367
		Expected Count	133,0	95,0	139,0	367,0
		% within ASSETS CLASS	36,2%	25,9%	37,9%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	35,294[a]	14	,001
Likelihood Ratio	38,235	14	<,001
N of Valid Cases	367		

a. 3 cells (12,5%) have expected count less than 5. The minimum expected count is 2,33.

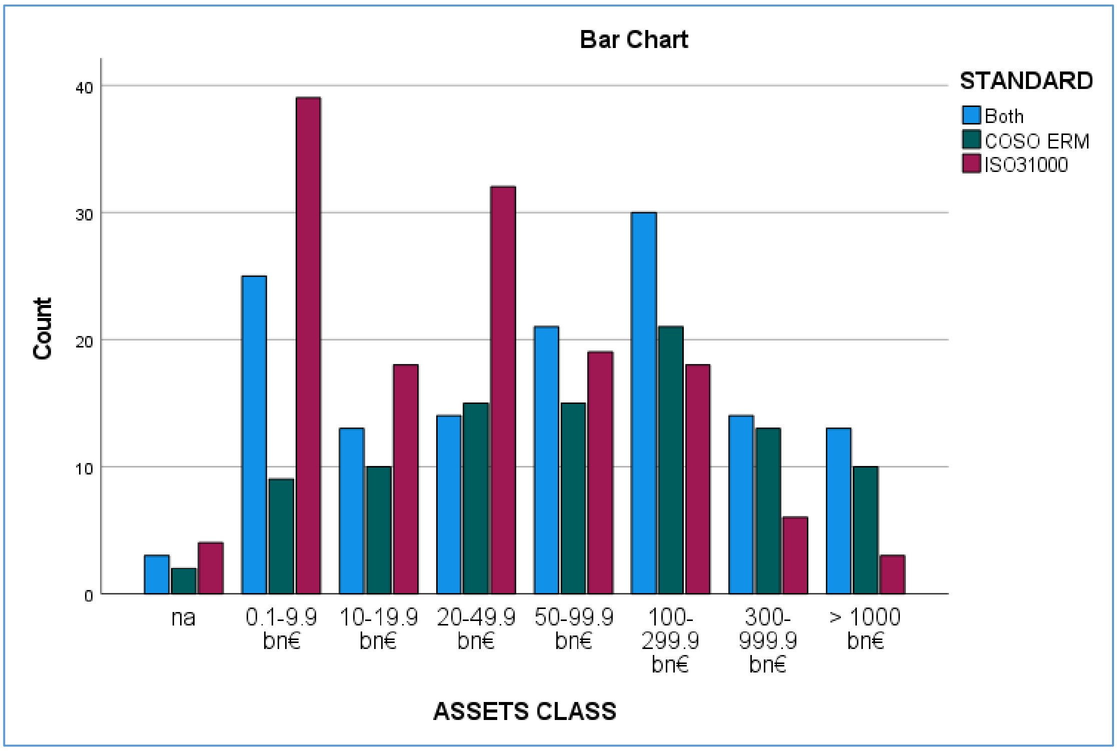


Symmetric Measures

		Value	Asymptotic Standard Error[a]	Approximate T[b]	Approximate Significance
Ordinal by Ordinal	Kendall's tau-c	-,200	,047	-4,254	<,001
N of Valid Cases		367			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.



From the crosstab, we can conclude the following:

- Smaller companies (with assets between 0.1-9.9 bn€), do not prefer COSO framework, but rather ISO 31000.

- Entities with assets between 20-49.9 bn€ also prefer ISO 31000.

- As the size of the entities increases, the preference to COSO or BOTH standards increases in values higher than the expected, with proportional decrease of observed ISO 31000 applications.

These initial conclusions are confirmed in the Chi-Square Tests Table, where X^2 is calculated and which has an asymptotic significance level of $p<0.05$, which proves that we have to reject the hypothesis of independence of the 2 variables.

The next Symmetric Measures table calculates the Kendall's tau parameter and we see that it has a Kendall's tau-c value (suitable for non-symmetric tables) $\tau= -0.2 <0.3$ which means there is a weak negative correlation between the 2 variables. This can be interpreted in a manner of "as the SIZE of the entity increases, the STANDARD variable moves (weakly) from ISO to BOTH"

All the above are visualized in the corresponding bar graph.

7.4 Discussion of the results

Focusing on the main and secondary objectives of our research, the results from processing of the sample data on the applicability and prevalence of either ISO 31000 or COSO ERM standards according to specific characteristics of the observed entities, demonstrate that:

- ISO 31000 is more popular across companies around the globe, than COSO ERM. Yet, there is a big percentage (36.2%) that apply BOTH frameworks.

  Comment: The fact that ISO 31000 appears more popular than COSO ERM was rather expected (see for instance the introduction of Chapter 6), but the application of both frameworks in a big portion of entities was not anticipated, since there were not relative references in the literature.

- As far as the COUNTRY of origin of the surveyed entities is concerned:
  - 15.5% are from USA and an additional 13.6% from Australia and New Zealand. These 3 countries with UK, Japan, Germany and France constitute 44.4% of the total sample, followed by China and Taiwan (an additional 7.1%).

- ECONOMIC SECTORS that are more eager and sensitive to apply risk management frameworks are "Banking and Financial Services", as well as

"Telecommunications", "Technology/Electronics" and "Oil & Gas Exploration & Production"

Comment: These outcomes are consistent with the references found in literature review and indicate the increased risk management culture of these industries.

- STANDARD variable correlates with the SIZE variable:
  - Smaller companies (with assets between 0.1-9.9 bn€), do not prefer COSO framework, but rather ISO 31000.
  - As the SIZE of the entity increases, the STANDARD variable moves (weakly) from ISO to COSO and finally to BOTH

  Comment: The fact that smaller entities have a preference for ISO 31000 rather than for COSO ERM was anticipated, since ISO is more structured and simple, therefore easier to implement and follow up.

- STANDARD variable correlates moreover with the CONTINENT and/or COUNTRY variables:
  - Australian entities prefer to apply BOTH standards
  - African entities apply solely ISO 31000

    Comment: Although, we intensively investigated for any clues of an African company that applies (or claims to apply) COSO ERM, we could not find any through our internet research. This outcome as solid as it may be, by all means reveals that COSO is definitely not popular in this continent.

  - European companies have balanced applications of either ISO 31000, or COSO or BOTH frameworks.
    - UK and SWEEDEN prefer ISO 31000
    - GERMANY and ITALY prefer COSO
    - SWITZERLAND applies BOTH

Comment: This outcome may be regarded as a finding, since there were not many applications in European entities in the literature review.

- Asian companies prefer either ISO 31000 or COSO but are very reluctant to apply BOTH. This is due to the fact that JAPANESE companies prefer ISO 31000, while CHINESE prefer COSO.

- In American continent, there is a preference for BOTH frameworks, mainly due to the specific trend in USA. Yet, there is a smaller but balanced number of applications of either ISO 31000 or COSO (mainly in BRASIL and MEXICO, respectively).

  Comment: Although not based on any literature review reference, US entities were expected to apply mainly COSO, due to the origin of the standard. Nevertheless, it seems that US entities chose to apply both standards.

- The ECONOMIC SECTOR of the entity does not correlate with the applied STANDARD. Yet, there are trends appearing in some specific sectors as:

  - For COSO in Banking & Financial Services and Insurance industries

    Comment 1: One would expect that ISO31000 would be more preferred by banks than COSO, based on the empirical results of previous surveys (see paragraph 5.1). In that view, this finding on the specific sample is new and should be an issue for further research in the future.

    Comment 2: The fact that insurance industry follows the same approach to risk management as banking industry is rather expected, since both sectors being financial services are subject to similar regulations and directives by supervisory authorities, hence have developed similar risk management cultures.

  - For ISO 31000 in Professional services and auditing and Telecommunications

    - For BOTH frameworks in Aerospace industry, Electric utilities, Pharmaceuticals and Postal Services & Logistics

- Two states (Australia and Canada) officially comply with ISO 31000 to all their governmental activities, while additional 2 commonwealth funds of the Australian state comply with BOTH standards.

It is essential, at this point to underline once again that it should not escape the attention of the reader that neither ISO 31000, nor COSO ERM are officially certifiable, giving room to surveyed entities to claim application and conformity to the standards without essentially following the respective processes, fostering the appropriate risk management culture or auditing their correct use.

CHAPTER 8. CONCLUSIONS AND FURTHER RESEARCH

8.1 Conclusions

One of the main goals of risk management is to foster a risk management culture within an organization. This involves instilling an understanding among employees and stakeholders of the significance of identifying, monitoring, and managing risks. Such a culture recognizes the value of proactive risk management and encourages individuals to take ownership of risk management processes. When a risk management culture is established, it can help to reduce the likelihood of negative events occurring, enhance organizational resilience, and ultimately contribute to the achievement of strategic objectives.

Managing a risk portfolio is a complex task, and there is no single approach that is universally applicable. Two commonly used frameworks for enhancing Enterprise Risk Management (ERM) practices are the COSO ERM framework and ISO 31000. However, one framework is not inherently superior to the other, and organizations should assess both to determine which aligns best with their unique culture and requirements, or if a combination of both is necessary.

COSO ERM is a comprehensive and intricate framework that may appear daunting to implement fully. On the other hand, ISO 31000 is simpler to understand and includes step-by-step descriptions of risk management procedures, along with practical guidance on how to incorporate risk management into decision-making processes. Additionally, ISO 31000 provides performance criteria that can help organizations gauge the effectiveness of their approach to risk management, making it a useful tool for those seeking a checklist for an ERM initiative or those with experience in other ISO-based management systems.

However, while ISO 31000 provides a good foundation, COSO ERM has valuable ideas and recommendations that can supplement it. By starting with an analysis of an organization's business objectives and strategies, COSO ERM can assist senior management in defining their risk tolerance and understanding the associated risk mitigation strategies. Furthermore, COSO ERM has released documents that apply its principles to specific areas such as cloud computing and compliance risk management. Thus, a combination of ISO 31000 and COSO ERM's relevant risk management principles may be the most effective approach.

Regardless of the framework used, it is important to evaluate the effectiveness of an ERM system over time to ensure that it aligns with the organization's business strategy, plans, and performance. If the ERM program is hindering business activities in any way, adjustments should be made to address the source of the friction. Organizations should be dynamic and regularly assess and adjust their ERM initiatives to manage risks appropriately.

The topic of application of ISO31000 and COSO ERM in real-world case studies has attracted the interest of the scientific community in the recent years, and several related scientific papers have been published.

Subject of this thesis is the critical evaluation of these 2 prevailing standards in risk management, as well as the field research of their applications in companies worldwide.

The sample we use consists of 367 entities (companies and state agencies) worldwide and it was obtained out of extensive internet search in various search engines, scientific databases, companies' websites, annual financial or management reports, press releases, articles, references in social media like LinkedIn.

The main conclusions of our research, as derived from the statistical analysis of the specific sample are the following:

1) Popularity of the standards: ISO 31000 is more popular across companies around the globe, than COSO ERM. Yet, there is a big percentage (36.2%) that apply BOTH frameworks.

2) Location effect: There is statistically significant proof that there are patterns of preference of one (or both) of the standards, related to the country of origin of the entity: a) U.S and Australian entities prefer to apply both standards, b) African entities apply solely ISO 31000, c) Asian companies prefer either ISO 31000 (as in Japan) or COSO (for example in China), but are very reluctant to apply both.

3) Sector effect: The vast majority of the sampled entities operate in the "Banking and Financial Services" sector (25.9%), followed by "Telecommunications" sector (10.1%), "Technology/Electronics" and "Oil & Gas Exploration & Production". This can be regarded as a result of the risk averse culture of these industries. There does not seem to be solid statistical evidence on specific preference of a standard according to the sector.

4) Size effect: The size of a company is essential in the choice of the standard, since statistical evidence show that smaller companies (with assets between 0.1-9.9 bn €) prefer ISO 31000 and as the size of the company increases more applications of COSO are recorded. Very large capitalization companies (assets > 1 tr €) choose to apply both standards.

5) Two states (Australia and Canada) officially comply with ISO 31000 to all their governmental activities, while additional 2 commonwealth funds of the Australian state comply with BOTH standards.

8.2 Issues and Limitations

Aim of this study is both to describe and analyze ISO 31000 and COSO risk management frameworks, as well as to research their applications in entities worldwide.

Regarding the second objective, that has been conducted by sampling a number of 367 organizations and enterprises, there are certain concerns and limitations that have been pointed out throughout the text.

Main reason of these concerns is that there do not exist registry databases of entities applying the two standards (not even partial or local), since neither ISO 31000, nor COSO ERM are officially certified.

Several problems arise from this fact, such as:

(i) A claim or statement that an entity applies or endorses one or the other standard may be challenged as just publicity/marketing material. Moreover, it does not necessarily mean that they comply with the full scope of the standard.

(ii) Introduction of one of the two standards in an entity does not necessarily mean that it continuously complies with it in the following years, since there is no regular external auditing, as is the case with other certifiable standards.

(iii) Any sample (including the one in hand) collected by internet research may suffer of representativeness and/ or bias.

The above indicate that there is a degree of uncertainty associated with our findings, and that there may be real variations or deviations from the outcomes of the analysis. Therefore, it is important to exercise caution when interpreting and utilizing the results, and to acknowledge the potential for error or variability.

8.3 Suggestions for Further Research

Future scientific research on the application of ISO 31000 and COSO ERM standards in organizations and enterprises, should consider the following directions:

- Formation of an official registry of applications worldwide.
- Inclusion and investigation of additional factors that may affect the choice/preference of a specific framework, such as headcount of the entity, capacity and structure of the risk management function, types of risks faced etc.
- Follow up of existing applications to identify potential problems encountered, variations from the standard's concept that have arisen over time, expansion across business lines, stakeholders' experience etc.

REFERENCES

- Alijoyo A., Norimarna S. (2021), "Risk Management Maturity Assessment based on ISO 31000 – A pathway toward the Organization's Resilience and Sustainability Post COVID-19: The Case Study of SOE Company in Indonesia", Proceedings of The 3rd International Conference on Management, Economics and Finance, DOI: https://www.doi.org/10.33422 /3rd.icmef.2021.02.134

- Alijoyo F. A. (2022), "The use ISO 31000:2018 in Indonesian Fintech Lending Companies: What Can We Learn?", Journal of Business and Management Studies, 4(1), 16–22, https://doi.org/10.32996/jbms.2022.4.1.3.

- Asmarawati S., Pangeran P. (2021), "ISO 31000-Based Risk Management and Balanced Scorecard to Improve Company Performance: A Case Study at Indonsian YNK Tour and Travel Company", International Journal of Multicultural and Multireligious Understanding 8(3):376, DOI: 10.18415/ijmmuv8i3.2341.

- Aven T. (2016), "Risk assessment and risk management: Review of recent advances on their foundation", European Journal of Operational Research, 253, 1-13.

- Basel Committee on Banking Supervision (2001), "Consultative document: operational risk", Retrieved from https://www.bis.org/publ/bcbsca07.pdf.

- Basel Committee on Banking Supervision (2004), "International Convergence of Capital Measurement and Capital standards. A Revised Framework", https://www.bis.org/publ/bcbs107.htm.

- Basel Committee on Banking Supervision (2010), "Basel III: International framework for liquidity risk measurement, standards and monitoring", https://www.bis.org/publ/bcbs188.htm.

- Beasley, M. S., Branson, B. S., & Hancock, B. V. (2010), "Developing Key Risk Indicators to Strengthen Enterprise Risk Management – How Key Risk Indicators can Sharpen Focus on Emerging Risk", Retrieved from https://www.coso.org/Shared%20Documents/COSO-Key-Risk-Indicators.pdf

- Bosetti L. (2015), “Risk Management Standards in Global markets”, 3rd Virtual Multidisciplinary Conference Slovakia, Vol 3, DOI: 10.18638/quaesti.2015.3.1.201

- CGMA-Chartered Global Management Accountants (2013), “Essential Tools for management accountants”, https://www.cgma.org/resources/tools/ essential-tools.html

- COSO - Committee of Sponsoring Organizations of the Treadway Commission (2017), “Enterprise Risk Management. Integrating with Strategy and Performance. Executive Summary”, https://www.coso.org/sitepages/guidance-on-enterprise-risk-management.aspx?web=1

- COSO - Committee of Sponsoring Organizations of the Treadway Commission (2020a), “Risk Appetite – Critical to Success”, https://www.coso.org/SharedDocuments/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

- COSO - Committee of Sponsoring Organizations of the Treadway Commission (2020b), “Compliance Risk Management: Applying the COSO ERM Framework”, https://www.coso.org/SitePages/2020-11-11---Compliance-Risk-Management--Applying-the-COSO-ERM-Framework.aspx

- COSO, Deloitte (2021) “Applying the COSO Framework and principles to help implement and scale Artificial Intelligence”, https://www2.deloitte.com/us/en/pages/audit/articles/applying-enterprise-risk-management-to-artificial-intelligence.html

- Deloitte (2019), “The future of operational risk management. Evolving Data Architectures”, https://www2.deloitte.com/content/dam/Deloitte/us/ Documents/regulatory/predictive-analytics-in-the-operational-risk-framework.

- Dias A. (2018), “ISO Standards Applicability and a Case Study About ISO 31000 in a Portuguese Municipality. American Journal of Theoretical and Applied Business. Vol. 4, No. 4, 2018, pp. 102-111. doi: 10.11648/ j.ajtab. 20180404.11.

- Ferreira S. & Dickason-Koekemoer Z. (2019), “A conceptual model of operational risk events in the banking sector”, Cogent Economics & Finance, 7:1, 1706394, DOI: 10.1080/23322039.2019.1706394.

- González L.O., Santomil P.D., Herrera A.T. (2020), “The effect of Enterprise Risk Management on the risk and the performance of Spanish listed companies”, European Research on Management and Business Economics, Volume 26, Issue 3, Pages 111-120.

- Govender D. (2019), “The use of the risk management model ISO 31000 by private security companies in South Africa”, Security Journal 32, 218–235, https://doi.org/10.1057/s41284-018-0158-x. [CrossRef]

- Greenbaum S, Thakor A., Boot A. (2019), “Chapter 6. Liquidity Risk” in “Contemporary Financial Intermediation”, Academic Press, pp 121-129.

- Haddad H., Laghzaoui F. (2020), “Review of Risk management standards: Convergences and divergences”, MJQQR Vol 2 Nr 1, ISSN 2665-8623.

- Hamir H., Sum R. (2021), “An Analysis of Risk Management Processes and Comparison with ISO31000:2018”, Asian Journal of Research in Business and Management, v. 3, n. 4, p. 16-30.

- International Standards Organization (2018), “ISO 31000: Risk Management Guidelines”, www.iso.org.

- IRM – Institute of Risk management (2022 retrieved), “From the cube to the rainbow double helix: a risk practitioner’s guide to the COSO ERM Frameworks”, https://www.theirm.org/news/from-the-cube-to-the-rainbow-double-helix-a-risk-practitioner-s-guide-to-the-coso-erm-frameworks/

- IRM – Institute of Risk management (2022 retrieved), “Standard Deviations: A Risk Practitioner Guide to ISO 31000”, https://www.theirm.org/news /standard-deviations-a-risk-practitioner-guide-to-iso-31000/

- Kumar S. (2022), “Risk Management Framework”, Available at SSRN: http://dx.doi.org/10.2139/ssrn.4141546.

- Læssøe H. (2022), “Prepare to Dare”, Books on Demand, Denmark.

- Lalonde C., Boiral O. (2012), "Managing risks through ISO 31000: A critical analysis", Risk Management. 14. 272-300. 10.1057/rm.2012.9.

- Mikes A., Kaplan R.S. (2015), "When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management", Journal of Corporate Applied Finance, 27(1), 37-40.

- Nilsen T, Aven T. (2003), "Models and model uncertainty in the context of risk analysis", Reliability Engineering & Systems Safety, 79, 309–17.

- NIST_National Institute of Standards and Technology (2012), "Guide for conducting Risk Assessments", Special Publication 800-30, csrc.nist.gov/ publications/detail/sp/800-30/rev-1/final.

- NIST_National Institute of Standards and Technology (2018), "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy", SP 800-37 whitepaper, https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

- Norlita W.A., Rarasati A.D. (2019), "Risk Analysis of Microfinance Conversion Based on ISO 31000 PT. Bank BRI Syariah. Tbk Aceh", RSF Conference Series: Business Management and Social Sciences e-ISSN 2807-5803/p-ISSN 2807-6699, Volume 1 Number 5 (2021): 125-134

- Nugroho, R. L. and Pangeran, P. (2021), "Improving the performance of a balanced scorecard through implementing ISO 31000 Risk Assessment at SHOFA pharmacy", EUREKA: Social and Humanities, (1), pp. 23-36. doi: 10.21303/2504-5571.2021.001635.

- Padro F. (2015), "Which is better for embedding risk management in higher education quality assurance: ISO 31000 or the COSO framework?", Proceedings of the 18th QMOD-ICQSS international conference on quality and service sciences, DOI 10.13140/RG.2.1.3247.8166.

- Pagach D., Warr R. (2010), "The Effects of Enterprise Risk Management on Firm Performance", Available at SSRN: https://ssrn.com/abstract=1155218 or http://dx.doi.org/10.2139/ssrn.1155218.

- Pham I. (2018), “Coso ERM and cyber risks in oil and gas industry”, Petrovietnam Journal, 6, 71-74. Retrieved from http://www.tapchidaukhi.vn /index.php/TCDK/article/view/369.

- Purdy G. (2010), “ISO 31000: 2009 –Setting a new standard for risk management”, Risk Analysis 30 (6) : 881 – 886

- Rahman A., Al-Dhaimesh O. (2018), “The effect of applying COSO-ERM model on reducing fraudulent financial reporting of commercial banks in Jordan”, Banks and Bank Systems, 13(2), 107-115, doi:10.21511/bbs.13(2).2018.09.

- Rubino M. (2018), “A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance”, International Journal of Business and Management; Vol. 13, No. 12.

- Safitri R., Pangeran P. (2020), “Balanced Scorecard and ISO 31000, Risk Management Integration to Improve Performance: Case Study at Indonesian Credit Union”, International Journal of Multicultural and Multireligious Understanding 7(6):527, DOI: 10.18415/ijmmu.v7i6.1802

- Schulte, J., Hallstedt, S. (2017). “Challenges for integrating sustainability in risk management – current state of research”, Proceedings of the 21st International Conference on Engineering Design (ICED17). Vancouver, pp. 327–336.

- Shayb H.A. (2021), “How COSO ERM and SHIModel algorithm can contribute to the development of enterprise performance”, Journal of Social Sciences 4(2), ISSN 2587-3490.

- Suyasa G.W, Legowo N. (2019), “The implementation of system enterprise risk management using framework ISO 31000”, Journal of Theoretical and Applied Information Technology Vol.97. No 10

- Syahputri H.Y., Kitri M.L. (2020), “Enterprise Risk Management Analysis of Group XYZ Based on ISO 31000:2018 Framework”, Asian Journal of Accounting and Finance, Vol 2 No 3.

- Tjahjono, Budiyanto, Khuzaini (2022), “Risk management at Rural bank with ISO 31000 approach”, Proceeding 2nd International Conference on Business & Social Sciences (ICOBUSS), Surabaya, March 5-6th, 2022.

- Toma S.V., Chitita M., Sarpe D. (2012), “Risk and Uncertainty”, Procedia Economics and Finance, 3, 975-980.

- Tumenbayeva O., Zhaksybekova G. (2016), “Implementation of the Integrated System of Risk Management in the Banks of Kazakhstan”, Indian Journal of Science and Technology, DOI: 10.17485/ijst/2016/v9i5/87607, Volume: 9, Issue: 5, Pages: 1-8.

- Van Greuning H., Brajovic Bratanovic S-S (2017), “Market Risk Management”, WorldBank e-Library, https://doi.org/10.1596/978-1-4648-1446-4_ch10.

- Wahyuni R.S. (2021), “COSO ERM Framework as the Basis of Strategic Planning in Islamic Banking”. Journal of Finance & Banking, Volume 25, Issue 1, page. 21-35ISSN: 1410-8089 (Print), 2443-2687 (Online)

- Wicaksono A.Y. (2020), “Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division”, International Journal of science, engineering, and information technology, Volume 04, Issue 02.

- Yalcintas A. (2013), “The Problem of Epistemic Cost: Why Do Economists Not Change Their Minds (About the "Coase Theorem")?”, The American Journal of Economics and Sociology, Vol. 72, No. 5, pp. 1131-1157.

- Καλφάογλου Φ. (1999), “Υποδείγματα μέτρησης πιστωτικού κινδύνου”, Δελτίο της Ένωσης Ελληνικών Τραπεζών Τεύχος Α’/99, σελ. 82-94.

- Λελεδάκης Γ. (2007), “Ανάλυση και διαχείριση χαρτοφυλακίου”, Εκδόσεις Οικονομικού Πανεπιστημίου Αθηνών.

- Τσάντας Ν., Μωυσιάδης Χ., Μπαγιάτης Ν., & Χατζηπαντελής Θ. (1999). “Ανάλυση Δεδομένων με τη βοήθεια στατιστικών πακέτων SPSS, EXCEL, και S-Plus”, Εκδόσεις ΖΗΤΗ.

- Χαλικιάς Μ. (2022), “Ποσοτική Ανάλυση και Στοιχεία Θεωρίας Αποφάσεων στη Διοίκηση και Οικονομία με Χρήση Λογισμικών EXCEL, ISALOS και SPSS”, BROKEN HILL PUBLISHERS LTD.