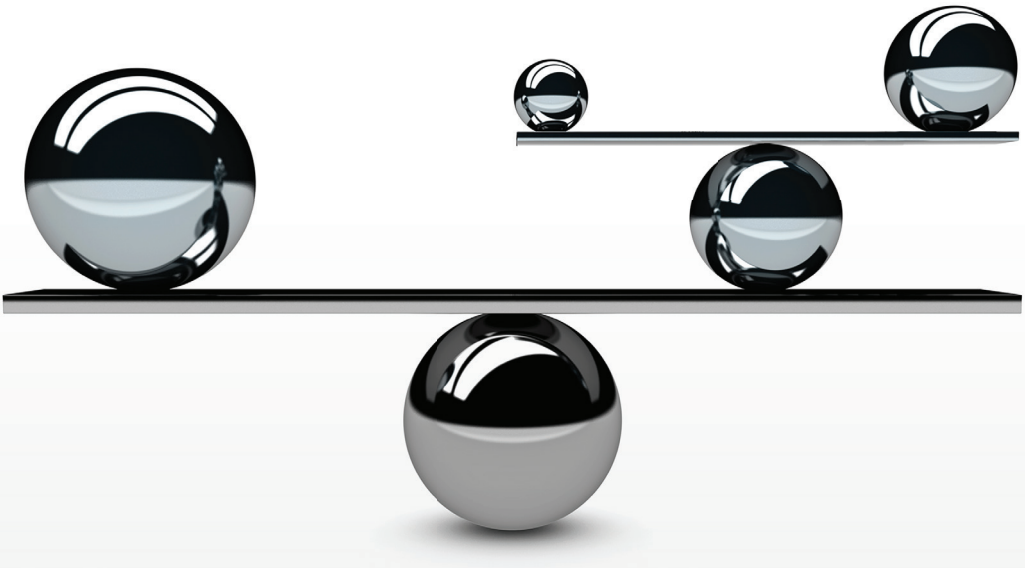
Business Law and Corporate Risk Management Collection
John Wood, *Editor*

HOW NEW RISK MANAGEMENT HELPS LEADERS MASTER UNCERTAINTY



Robert B. Pojasek, PhD

BEP BUSINESS EXPERT PRESS

How New Risk Management Helps Leaders Master Uncertainty

Robert B. Pojasek, PhD

BEP BUSINESS EXPERT PRESS

How New Risk Management Helps Leaders Master Uncertainty

First published in 2019 by
Business Expert Press, LLC
222 East 46th Street, New York, NY 10017
www.businessexpertpress.com

ISBN-13: 978-1-94999-160-4 (paperback)
ISBN-13: 978-1-94999-161-1 (e-book)

Business Expert Press Business Law and Corporate Risk Management Collection

Collection ISSN: 2333-6722 (print)
Collection ISSN: 2333-6730 (electronic)

Cover and interior design by Exeter Premedia Services Private Ltd., Chennai, India

First edition: 2019

10 9 8 7 6 5 4 3 2 1

Printed in the United States of America.

Abstract

Risk is the effects of uncertainty on the ability of an organization to meet its strategic objectives. The effects of uncertainty are expressed as opportunities and threats. Most people associate risk with hazards and losses (i.e., pure risk). Unlike pure risk, uncertainty risk is not insurable because of its upside risk opportunities. These opportunities are identified by scanning the internal and external operating environments of an organization. Highly ranked opportunities can be developed to help offset the threats to the organization. Risk management is a key element of the open-sourced, "high-level structure" developed by the International Organization for Standardization. This structure for managing important organizational programs has been adopted by over 180 country standard-setting organizations.

The high-level structure accountability for risk management has been assigned to an organization's "top leader." This concise book provides the information needed by that leader to identify opportunities and threats and decide on the appropriate risk response in an uncertain world. The two most widely used risk management standards are presented to demonstrate that an organization can use either one or a combination of the two standards to help manage the effects of uncertainty on the organization. Some organizations use this information to create a risk management program that is unique to their organization. It is fool worthy to attempt to run an organization without formal uncertainty risk management. Let this guide help you find your way in this uncertain world.

Keywords

High-Level Structure; Risk; Risk Management; Opportunities and Threats; Organizational Objectives; COSO ERM:2017 Enterprise Risk Management Standard; ISO 31000:2018 Risk Management Standard; Top Leader's Accountability

Contents

Reviewers Notes

Wayne Muscarello

This book is exactly what I would expect to read if I were an executive. It clearly lays out the terms of risk management, provides a baseline understanding of the components of risk management and offers a reference to the tools that should be used.

The flow of the information in the book is written to guide you through the entire process in order. The material provides the reader with a background on risk management which adds a bit of interest to the subject matter.

The thing I liked best about the book is the concise information the user of presented in bullet points to easily allow the reader the ability to pull the information into a slide deck for a presentation. Plus, it allows the reader to quickly find the information.

The processes and information in the book are exactly what is used in most organizations today. It's current and relevant to how large and small organizations function. Experienced risk managers will know that the information captured in the book is indicative of how risk management is implemented at most organizations.

Most executives in the United States are more familiar with COSO than the ISO standards. The book gives them reinforcement on COSO and possibly the first glimpse of what ISO 31000:2018 is about. The CRO of a company would easily see how useful the information is and could effortlessly pull text from the chapter to create slides for a presentation.

I don't know of any company that has formal risk management competency requirements for any staff except IA (Internal Audit). The book reminds organizations to add some type of risk competency and awareness for employees as part of the onboarding process.

Lawrence Heim

The book offers a detailed analysis of integrating the ISO 31000:2018 risk management system and the COSO ERM: 2017 enterprise risk

management system into company operations and management. Dr. Pojasek's comparison and contrast of ISO 31000 and the more familiar COSO framework gives helpful and practical tips for integration or establishing an enterprise risk management standard from the information derived from the two standards.

Ralph Jarvis

Dr. Robert Pojasek is a pragmatic thought leader in sustainability and integrates sustainably developed principles into corporate business practices. This book flows easily, directly and connects from the top level to the next levels. It conveys a logical step-by-step approach for implementing risk management within the high-level structure used today by the top corporations around the world. Each topic emphasized is interwoven and relates to themes previously discussed. It provides the reader a signal to revisit those chapters to refresh their understanding. Dr. Pojasek demonstrates an effective model identifying and illustrating the international risk management methods. But don't be surprised when he expands other related insights and underpinnings, as well!

Preface

Many people believe that "risk" only has negative consequences. While this is true with "pure risk," you will learn that "context risk" addresses the "effects of uncertainty" with potential adverse effects (threats) and potential beneficial effects (opportunities). Every organization experiences both kinds of risk. They manage pure risk with the help of insurance and the placement of "controls" on the operations. Context risk involves the searching of the external and internal environments of the organization for "opportunities and threats." Context risks are managed with standards, such as COSO ERM:2017 and/or ISO 31000:2018. These copyrighted standards are designed to help an organization's leader decide "what" they need to do in order to conform. However, more importantly, the standards often suggest "how" the organization can meet the standard.

In this book, we present the clauses in the standard that describe the "what." This information can be found on the Internet since both standards have published open source summaries of the standards. This concise book strongly recommends that the top leader purchase the standards (see the book list provided in Chapter 2) to determine how to best determine the options (the "how") for implementing the standards in their organization. The limited use of information from the standards has been cited in text with endnotes provided for each chapter. This should help the reader identify the complete citation that can be found in the references. "Fair Use" also allows this book to support risk management courses taught at the master's degree level.

The first chapter in this book should help the reader understand the many topics and perspectives involved in when someone is evaluating different kinds of risk in the organization. In the second chapter, the reader will learn about risk management. It only deals with context risk and the "effects of uncertainty." Pure risks are "controlled" to manage risk and contain the costs of insurance.

Chapters 3 to 5 examine how ISO 31000:2018 systematically addresses opportunities and threats in an organization. This standard has

a well-defined implementation approach. Sections of COSO ERM:2017 are presented that work quite well in tandem with ISO 31000:2018. These standards are rarely integrated with each other. Information in these chapters will enable the reader to use a purchased copy of the standards for creating a risk management program that works best for the organization.

Chapter 6 examines the remaining sections of COSO ERM:2017 and how they can be used in addition to ISO 31000:2018. Your organization now has a choice. It can use either standard, integrate the two standards, or use both standards to construct a unique risk management method that will work best for your organization.

Chapter 7 examines how risk management can be used with the ISO "high-level structure" that is used in all the ISO management systems. This high-level structure is an open-source document available on the Internet. Besides allowing organizations to integrate standards to have all the information in one place, they also offer a means for integrating risk management into the work that everyone does every day within the organization where they work.

No matter what direction is chosen, the person designated as the "top leader" of the organization should purchase the two standards. As stated earlier, these standards are written to provide useful copyrighted information on *how* best to use the standards. This is a big step beyond understanding *what* can be done with these two risk management standards. The standards provide much more detail than is presented in this concise book. You can locate the organizations that sell these two standards on the Internet. In Chapter 2, I have suggested a reading list on risk management for the top leader of an organization. This list is helpful since the ISO high-level structure holds the "top leader" fully accountable for obtaining objectives set by the organization. The responsibility of leadership to be held accountable for the use of risk management is highlighted in the additional readings that will help the organization move beyond the defensive posturing around different kinds of risk and the different ways that risk is managed. It will take a compelling vision of the "top leader" to overcome the indecisiveness and lead the way to a risk-aware culture that will be needed to find the opportunities that will help the organization offset the threats. Success is determined when the organization meets it strategic objectives that are derived from its mission statement.

I would like to thank the peer reviewers that provided clarity and new ideas that needed to be explored in this effort. They include:

- Lawrence Heim—ELM Sustainability Partners
- Ralph Jarvis—Jarvis Business Solutions LLC
- Charles Wayne Muscarello—IT Internal Audit Consultant

I would like to thank Tammy Wyche (Institute of Internal Auditors) for alerting me to the most recent COSO ERM:2017 standard and how risk management is currently used in internal auditing. John Wood, Esq. is an Editor for Business Expert Press. With his review and guidance, I was able to work with the editorial staff of Business Expert Press to complete this book so that you could use it with confidence to lead a risk management effort in your organization. I will host a microsite on this book at http://bringchangenow.com I will also publish new uses for the information in the book and engage in conversations with the people that are using the book and the outcomes of this work. Hopefully you will join in on that conversation and learn about specialized training that we will make available on the topic of risk and risk management.

Robert B. Pojasek, PhD
Strategic Impact Partners
Boston, MA USA
https://BringChangeNow.com

CHAPTER 1

Understanding Risk

Introduction

The Oxford Dictionary defines "risk" as a situation involving exposure to danger. Asking people for their definition of risk provides us with a variety of responses. Some of these responses focus on a concern for uncertainty or danger, while others refer to the financial consequences of unwanted events. Every organization faces some degree of risk every day. However, we normally focus on catastrophic events and whether the organization is properly covered by insurance protecting us from the consequences of these events.

Other sources of risk include the following[1]:

- The possibility of an unfortunate occurrence
- Doubt concerning the outcome of a situation
- Unpredictability
- Possibility of loss
- Needing to improve the ability to be an effective leader

These conceptions of risk help us understand risk broadly as the uncertainty of future events and their outcome for our organization.

Leading companies create or adopt frameworks for understanding risk and supporting risk management. Typically, the approach to understanding risk is one that supports the business and its internal and external context, while ensuring that risk management is embedded across the entire organization. This action requires an explicit management dialogue with every element of the organization and its key stakeholders. Generally, corporations do not like risk or uncertainty. In these organizations, new initiatives are carefully reviewed to either eliminate risk or mitigate that risk to levels acceptable to the organization. This situation makes these

companies more vulnerable to disruption as entrepreneurial companies have a greater tendency to put risk aside or accept a higher risk tolerance to make an impact on how organizations conduct their business.

As a result, it is important for organization leaders to understand risk and uncertainty. There are manageable ways to understand risk without having to get confused by all the risk-naming conventions. The organization should conduct a thorough search for risks as a first step in a risk management program. This list needs to be updated whenever changes in the company occur or when circumstances relevant to the organization changes (e.g., governmental changes, economic instability, social trends, etc.). It is not necessary to build a complicated risk classification system. The major risk management program standards do not encourage the classification of risk. A few important concepts necessary to understand risk are presented as follows.

Pure Risk and Speculative Risk

A pure risk features a chance of a loss and no chance of a gain. People often use the word "risk" to describe a financial "loss." Losses result from: fires, floods, snow, hurricanes, earthquakes, lightning, and volcanoes. Within the business, losses include more complex matters, such as sickness, fraud, environmental contamination, terrorism, electronic security breaches, and strikes.

A risk is the possibility of a loss. A peril is the cause of a loss. Perils expose people and property to the risk of damage, injury or loss against which the organization often purchases insurance to cover the cost of that loss. Please note that the terms peril and loss are often mistakenly used interchangeably.

Insurance companies cover financial losses from pure risks that meet conditions: due to chance; definitiveness and measurability; statistical predictability; lack of catastrophic exposure; random selection; and loss exposure.

PURE RISK involves a chance of a loss and no chance of a gain. Organizations generally use insurance to deal with pure risk. Operational controls are used to reduce the total cost of insurance.

Pure risk can involve a hazard. A hazard is something that increases the probability that a peril will occur (e.g., ice-covered road). Hazards are a condition or a situation that makes it more likely that a peril will occur. The situations include physical hazards, operational hazards, and business hazards. Common hazards include chemicals, repetitive motions, and physical conditions (e.g., vibrations; noise; slips, trips and falls; ergonomics); and biological effects.

Speculative risks are activities that produce a profit or a loss. These kinds of activities include new business ventures, reputation protection, modifications to operations, and alternative means of transportation. All speculative risks are undertaken as a result of a conscious choice. Speculative risk lacks many of the core elements of insurability.

Financial and Non-financial Risk

Larger corporations focus on the financial risk of their operations. Financial risk refers to an organization's ability to manage its debt and financial leverage. It also refers to non-debt financial losses, like lawsuits, property losses, crime/fraud and cyber risk. To address these financial risks, organizations create performance measures which include cash flow, credit, earnings, equity, foreign exchange, interest rates, liquidity and financial reporting.

However to have a vibrant risk management program in an organization, it is important to consider the non-financial risks associated with the operations. Non-financial risk are events or actions, other than financial transactions, that can negatively impact the operations or assets of a company. Typical non-financial risk (see Figure 1.1) includes misconduct, technology, ignoring key external stakeholders, customers and employees.

However, there are some drawbacks associated with non-financial performance measures. It is costly to have to monitor a large amount of financial and non-financial information. In some cases, the cost is greater than the benefits. Having many performance measures requires maintaining and studying information from multiple sources. There is often a competition between maintaining a good set of measures and finding the time needed to spend more time engaging with stakeholders and serving the customers.

There are established and certifiable means of measuring financial performance measures. However, this is not the case in non-financial

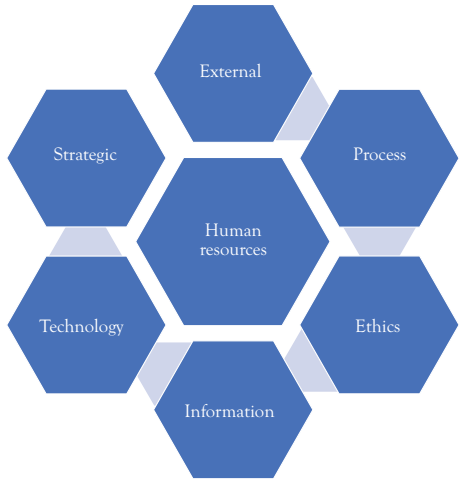


Figure 1.1 Non-financial risk[2]

measures. Evaluating performance or making tradeoffs between measurements is difficult when some are measured in time, others are measured in percentages or amounts, and a few are determined in arbitrary ways. Furthermore, not all stakeholders understand, or hold a similar appreciation of, non-financial measures. Lastly, accounting systems are designed around financial measures and do not handle non-financial concepts well. (see Figure 1.2).

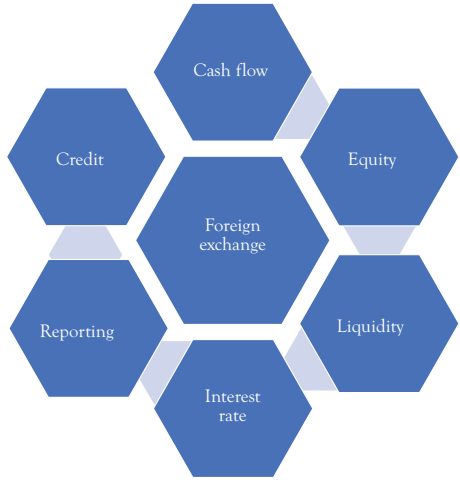


Figure 1.2 Financial risk[3]

Although non-financial measures are receiving more attention in risk management programs, organizations should not simply copy the measures from other organizations.[4] The choice of the non-financial measures should be unique to each company and linked to organizational strategy and meeting the organizations explicit objectives and other value drivers.

Opportunities and Threats

With the advent of the practice of risk management (i.e., different than hazards control) in the 1990s, there has been a shift to using opportunities and threats as a means of managing risks of an organization. As noted earlier, the traditional view of risk is negative. This view characterizes all risks as "threats" with adverse consequences on the ability of the organization to meet its objectives. However, there is a possibility that uncertainty in the internal and external operating environments can create an "opportunity" which has a beneficial effect on achieving organizational objectives. This is consistent with the more recent view of risk as being the "effects of uncertainty" on the ability of the organization to meet its business objectives. The nature of uncertainty and its effect on objectives can change over time. As a result, the risk will change. What is found in uncertainty today, may not be true in the future. Since most business strategic objectives are established for a five- to ten-year timeframe, it is very important to continuously monitor and measure the operating environment.

The International Organization for Standardization (ISO) defines "effect"[5] (as in the effects of uncertainty) as "a deviation from the expected—positive or negative." Opportunities that are brought to light are often not the opportunities that might have been already known to the organization. They are challenging opportunities, so the thought of them being a "risk" is very apropos. Most organizations that are using the opportunities and threats in their risk management program, select a couple of the highest ranked opportunities and seek to exploit them in lieu of simply treating the top threats that have been identified. It is important to remember that you should not use the word "risk" interchangeably with the word "threat."

Context Risk

The context risk is defined as follows[6]:

The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative, or both. An effect can arise as a result of a response, or failure to respond to an opportunity or to a threat related to objectives. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihoods.

Establishing the context of an organization is concerned with the understanding of the external and internal operating environments to identify the risks (i.e., opportunities and threats) that would be of concern to the company. The information obtained from determining the context risk will help identify the structure for the risk management activities described in Chapter 2. Careful delineation of the context risk is needed to[7]:

- Clarify the organization's objectives.
- Identify the operating environments within which the objectives are pursued.
- Specify the scope and objectives for the risk management, boundary conditions and the outcomes.
- Identify the criteria that will be used to measure the risks.
- Define a set of key elements that will be used to structure the risk identification and assessment process.

The context is used to establish, implement, maintain and continually improve the organization's high-level structure.[8] Creating an understanding of the context risks provides an appreciation of all the factors that could exert an influence on the ability of an organization to meet its objectives (i.e., outcomes). The organization determines those opportunities and threats that need to be addressed and managed.

Context Risk is the effects of uncertainty on the ability of the organization to meet its objectives. These risks consist of both opportunities and threats.
Risk management—coordinated activities to direct and control an organization with regard to risk.

External Context and Stakeholders

The external environment is part of the organization's context. It is anything, including the external stakeholders, in the external operating environment that can influence the organization's ability to achieve its objectives.[9] The PESTLE tool (an acronym of influences that stands for political, economic, sociological, technological, legal and environmental) provides a risk classification system for the external context.[9] There are large numbers of possible "factors" associated with each "influence" defined by the PESTLE tool. External risk comprises both opportunities and threats that are not wholly within the control of the organization. In some cases, the organization would have to work with external stakeholders to realize these opportunities and threats.

The PESTLE tool is not mentioned by name in the ISO 31000:2018 risk management standard. However, it is mentioned in the COSO ERM:2017[11] and in the Australian standard that was used in the process of writing ISO 31000:2018.[12]

PESTLE analysis is a widely used tool for searching for opportunities and threats associated with an organization and its supply chain. It creates a conversation about opportunities and threats that can work well to engage external stakeholders as required by ISO 31000:2018 and COSO ERM:2017. It is important to use a practice known as "sense making" so that information gathered during screening is clearly understood by those responsible for conducting the scanning activity and to help the survey team record this information in the knowledge management system.[13]

Every opportunity and threat catalogued by the PESTLE search team has an external stakeholder associated with it.[14] ISO 31000:2018 requires stakeholders to be directly involved in the risk assessment process. This helps engage these stakeholders as a front-line effort to keep the scanning of the external environment up to date at all times and to help the organization understand the significance of the factors found in each of the influences. These stakeholders can also help assess the "materiality" of opportunities and threats for the sustainable development program.

Internal Context and Stakeholders

The internal context can be determined by scanning the situation within the organization with a TECOP tool[15] (an acronym of influences that stands for technical, environmental, commercial, operational and political). This tool is widely used in the project management field.[16] Like the PESTLE tool, this TECOP scanning tool is designed to help understand the influences and factors (i.e., subset of activities within each influence) affecting the operation of the organization and to be able to identify the opportunities and threats associated with the factors.

SWIFT Tool

Many people responsible for characterizing the internal and external context use a "structured what-if technique" (SWIFT)[17] to ask questions that help find the "factors" and the opportunities and threats. This tool also has wide use for those working with hazard risks. By understanding the process, it is possible to create internal controls to lower the "pure risk" and support the risk management effort. The SWIFT tool involves the use of process maps to make sure that all the main processes and their supporting processes are covered both in the SWIFT activity and in the TECOP activity.

Strategy Risk

All organizations find themselves dealing with a wide range of uncertainties every day. The opportunities and threats associated with uncertainty may impact the organization's ability to execute its strategies and achieve its strategic objectives.[18] These opportunities and threats can ultimately affect shareholders' and/or stakeholders' view the long-term viability of the organization.

The organization's strategy (whether derived explicitly or implicitly) is the process to establish and maintain the strategic objectives of the organization. Failure of the strategy effort to manage opportunities and threats while establishing and maintaining objectives is just as important in having them impact the strategic objectives after they are created.

Leaders need to first think about the strategy that their organization is using to achieve its objectives. They can then use that knowledge to manage opportunities and threats that could potentially be significant enough to threaten the strategy and improve the ability to meet the objectives.

Strategic risks are very broad in practice. Most risk managers do not focus on strategic opportunities and threats. The focus should be on the exposure of the strategy in its ability to create the most important opportunities for the organization.

Risk and Risk Management Vocabulary

When dealing with risk in the context of an organization, it is important to share a common language regarding risk and risk management. The ISO has created an "open source document" for this purpose.[19] Some of the ISO management system standards slightly modify these terms. Company communications concerning risk management efforts must use an agreed upon vocabulary. The top leader should make sure that these terms are consistently used both within the organization and when seeking engagement with the stakeholders.

Hazard risks undermine objectives and often have a high level of significance in some industries. These hazard risks are closely related to insurable risks. Remember that a hazard (or pure risk) can only have a negative outcome. The occupational health and safety management system, ISO 45001:2018, is very careful in maintaining information on both hazard risk and the risk associated with the effects of uncertainty. Consider the wording in this standard's Section 6.1.2.2.[20]

"The organization shall establish, implement and maintain a process(es) to:

(a) assess OH&S risks from the identified hazards, while taking into account the effectiveness of existing controls;
(b) determine and assess the other risks related to the establishment, implementation, operation and maintenance of the OH&S management system."

All management systems will need to separate the hazard risks in a similar manner.

Upside of Risk

There are many ways to look at what people refer to as "the upside of risk." It can represent the potential to eliminate a degree of uncertainty by exploiting an identified opportunity. When successful, the organization would be ahead of its plan to meet its strategic objectives. By adding opportunities to the risk management definition, you would think that organizations would be embracing this chance to be on the upside of risk. But another explanation would have the organization undertake activities that it would not otherwise have the "appetite" to undertake. No matter how you think of the upside of risk, everyone can agree that this is a place that you wish to be.

Investors believe that when an organization accepts a substantial risk, there is chance that there could be a greater opportunity. The ISO management system standards have some problem with the use of risk in this phrase since it is assuming that the risk is equal to threat. To get around this point, the standards have redefined "risk and opportunity" to mean[21]: "potential adverse effects (threats) and potential beneficial effects (opportunities)."

While there are a lot of nuances associated with opportunities and threats, organization's will be seeking the ability to use opportunities to offset threats.

Documenting Risk

It is important to document each of the activities described in this chapter. Organizations used to maintain detailed "risk registers" with information on the risks that have been identified. However, this terminology was associated with tables and spreadsheets that are no longer in widespread use. Now companies maintain a "risk profile," with the risk identification process. This document provides a composite view of the risk assumed at a level of the organization, or aspect of the business, that positions management to consider the types, severity, and interdependencies of risks. It also states how these risks may affect performance relative to the strategy and objectives.[22]

The major tools used today for gathering information on opportunities and threats are the PESTLE and TECOP analyses. The information from these scans and the use of the SWIFT tool must be documented and reviewed by the top managers to assess the effectiveness of the risk management program. The concept and practice of risk management is presented in the next chapter.

Notes

1. Insurance Institute of Ireland (2014).
2. Baker (2018).
3. Baker (2018).
4. Ittner and Larcker (2000).
5. ISO (2015a).
6. ISO (2015).
7. Standards Australia, Standards New Zealand (2004).
8. ISO (2015).
9. COSO (2017).
10. Hopkin (2012).
11. COSO (2017).
12. Standards Australia, Standards New Zealand (2004).
13. Pojasek (2017).
14. Pojasek (2017).
15. Pojasek (2017).
16. Hillman (2014).
17. ISO (2009).
18. Anderson and Frigo (2014).
19. ISO (2009a).
20. ISO (2018a).
21. ISO (2015a).
22. COSO (2017).