



# 5 EFFECTIVE METHODS TO IDENTIFY RISKS IN YOUR ORGANIZATION

Tools, techniques, and best practices for  
identifying risks to company strategy and  
everyday operations



*Helping organizations protect value*

Carol Williams, CRM  
carol@erm insightsbycarol.com  
[www.ERMInsightsbyCarol.com](http://www.ERMInsightsbyCarol.com)

# TABLE OF CONTENTS

Introduction	2
Chapter 1: Risk Identification Basics and What to Expect	3
Chapter 2: Common Misconceptions and Missteps	8
Chapter 3: Five Risk Identification Methods and Choosing the Right One	14
Chapter 4: Conclusion and Final Thoughts	24
External Sources	25
BONUS: Risk Identification Methods Quick Reference Guide	26

# INTRODUCTION

Risk identification: it's not just the first step in the risk management cycle, it's the most important step. That's because risks cannot be managed unless they are first identified.

Simply having an ERM program in place isn't enough. Without a solid and methodical risk identification process, companies waste time and resources on trivial risks while neglecting the major ones. It's little wonder that these ERM programs fail to gain traction with executives and are eventually abandoned.

**Risk identification is the foundation for the entire risk management process.** No one in their right mind would build the walls of a house on uneven, bare ground, would they? That's why risk managers must account for all relevant activities and scenarios before moving on to the next step.

**The purpose of this guide is to help organizations of all sizes develop a methodical process for identifying risks, whether it's for the whole enterprise or within specific business units, projects, or activities.**

In the following pages, you will learn the basics of risk identification, some common misconceptions, who you should involve in the process, and how you can determine the level of success.

Start building a strong foundation for your risk management process today.

# CHAPTER 1: RISK IDENTIFICATION BASICS AND WHAT TO EXPECT

Risk identification is an activity that should be conducted periodically and on a continuous basis. Although both definitions below indicate that risk identification should be done monthly, quarterly, or yearly, author Norman Marks emphasizes in his book *World-Class Risk Management* that it should be a part of any decision being considered.

Marks explains: “Before an intelligent decision can be made, it is necessary to identify, analyze, and evaluate the risks (both positive and negative) that can happen for each option.”

The International Organization on Standardization (ISO) issued standard 31000, which is one of several types of risk management standards that organizations can use. The ISO standard defines the risk identification step and its goal as the following:

“The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity.



Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.”

Risk identification is important because it is used to create a list of risks the organization is facing. All of the subsequent steps in the risk management process are aimed at the same list of risks. Therefore, the value of entire process is contingent on the quality of the risk identification.

COSO, short for Committee on Sponsoring Organizations, refers to this step as “event identification” and defines it as follows:

“Management identifies potential events that, if they occur, will affect the entity, and determines whether they represent opportunities or whether they might adversely affect the entity’s ability to implement strategy and achieve objectives. Events with negative impact represent risks, which require management’s assessment and response. Events with positive impact represent opportunities, which management channels back into the strategy and objective-setting process. When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organization.”

One common thread between the ISO and COSO definitions is that they include risks with both negative and positive outcomes.

Most people define risks as potential events that can have a negative consequence to the organization. However, the risk identification process should also consider “positive” risks that could “enhance” the achievement of objectives or represent an opportunity for the organization.

As we explain in this [blog post](#), it's vital to identify positive risks or opportunities for two reasons: 1) While you may have a positive outcome in a particular situation, you may be creating risks elsewhere, and 2) Identifying opportunities can help ensure goals are met faster or with better results.

---

## WAYS YOU CAN USE RISK IDENTIFICATION

Many of the materials you will encounter in print or online about ERM focus on identifying risks to the company as a whole.

However, there are times when you will need to identify risks to a specific area or process. Examples can include:

- Strategic planning
- Business function
- Project
- Process
- Activity

Specific risk identification methods will be reviewed in-depth in Chapter 3. However, it is important to note that you can modify these techniques to fit the situation at hand. Be sure to document the overall objectives and scope of the inquiry and make sure everyone involved in the process understands these points.

---

## WHAT TO EXPECT AT THE END OF THE RISK IDENTIFICATION PROCESS

The risk identification process should produce a list of risks that may positively or negatively impact the organization. The enterprise must come

to an agreement as to which risks appear on the list and how those risks are worded. Typically, executives will want to see only the biggest risks to the organization, frequently called Top Risks.

The adoption of a common terminology can ensure everyone is engaged and working from the same information as you progress to the next step in the risk management process. Without this commonality, IT will use a different terminology than finance, which will lead to a stove piping of risk management within a business unit and not benefit the enterprise at a higher level.

Of course, a list is just a list until action is taken against it. Assuming your company's efforts have identified the correct risks, it's the *management* of those risks that ultimately "creates, protects and enhances shareholder value" as explained by Dr. Paul Walker on his blog at RiskAcumen.com. For a high-level discussion on managing risks, see my article on [common risk response strategies](#) for more.

## CHAPTER 1: AT A GLANCE

Risk identification is the process of identifying potential risks, including their sources and causes, where they may impact the organization, and the potential consequences.

Organizations should not only look for risks with negative consequences, but also “opportunities” or “positive risks.”

Risk identification needs to be done on a continuous and periodic basis and should be a part of any decision at any level.

The risk identification process is the beginning stage of developing a list of top risks to the organization.

Risk identification isn't just for company-wide concerns, but should also be used for processes, projects, and activities.



## CHAPTER 2: COMMON MISCONCEPTIONS AND MISSTEPS

Before examining the different methods organizations can harness to identify risks, it's important to discuss some of the common misconceptions and missteps that occur along the way.

Falling into to one of these traps could lead to a loss of executive support or a loss of interest among middle managers and front-line staff. Without engagement from the entire company, the ERM initiative will flounder and be seen as more of a nuisance than a value-enhancing endeavor.



While the risk identification process, and risk management in general, will involve some trial and error for every organization, the following could be disastrous for your company's risk initiatives.

- **Being reactive to a problem**

Waiting until something is a problem before addressing it is a common mistake for both individuals and organizations. In the context of risk, many companies will gloss over a subject because it simply isn't a pressing concern. However, risk management yields the most benefit when it is proactive—before the risk becomes an issue.

There are a couple of benefits of addressing a risk in advance:

- 1) If you take steps ahead of time to mitigate an industry-wide risk such as the financial crisis of 2008-09, and your competitors do not, your company can benefit through what's called a "survivor's bonus."
- 2) If your organization is better able to weather a storm than competitors, the board can factor this into the company's strategic planning.
- 3) The additional time allows for robust planning and resource allocation, so that the necessary people and money can be used to address the subject. This is a better option than telling your people to drop everything and focus on the problem due to lack of planning.

- **Not using a methodical approach to identifying risks**

You've probably been able to surmise by this point that risk identification involves more than just writing some risks down on a list. There are all sorts of methods to consider based on who you're reaching out to, the scope of the inquiry (i.e. company-wide, project, business unit), and more.

Being methodical, especially in this step of the risk management process, ensures a greater chance of identifying all important activities and possible risks and consequences to those activities. Failure to do so could lead to critical risks being overlooked and a loss of credibility to the program. And taking a haphazard approach will not gain the confidence and support needed for a successful risk management program.

- **Not viewing a risk within the larger context of the organization**

Simply viewing a risk within the lens of a particular business unit is probably the most common pitfall of the risk identification process. Doing so negates the whole purpose of *enterprise* risk management.

Risk identification for ERM isn't simply identifying a risk and addressing it within the business unit, but rather examining its impacts to other business units, the organization's strategy, and more. For example, if you identify a risk in the IT Department and only take steps to address it within that silo, you may end up creating new risks for the Financial Department.

This is one of the core reasons why it's important to involve cross-functional leaders from different functions within the company (i.e. IT, legal, finance, marketing, etc.). Having the collective expertise of the organization at the table ensures you're not "stove-piping" your risk identification efforts.

- **Identifying a risk without understanding scope**

During the risk identification process, it is common for managers and directors from a specific business unit to emphasize risks to their area. For their particular area, it very well may be a significant risk.

It is important for the risk management team in conjunction with other business areas to take a step back and think about whether a particular risk is significant to the company as a whole and its objectives. Although a risk may seem significant to a single business unit, it may only be a minor issue when viewed through a larger lens or after being aggregated into the larger list. The risks identified as impacting multiple areas, or pervasive risks, are likely going to be higher risks to the company than single business area risks. Prioritize efforts on those pervasive risks. Not taking this step will

cause you to squander time and resources on risks that are insignificant in the long run, which could trigger a decrease in executive buy-in.

- **Not tailoring the risk identification process to your organization or the participants**

Although connected to taking a methodical approach to risk identification, this particular pitfall warrants its own section since so many organizations simply use the same approach for everyone within the company. However, failure to tailor the process to the company's culture and who you are talking to can cause resistance, confusion and ultimately a failed process.

For example, you wouldn't want to use a detail-oriented approach when engaging with a busy executive or the interview approach when soliciting input from a large pool of people. However, if you are speaking with executives on a more strategic level, an interview may be the better option to ensure you capture all of the information you need to. If the company's operations are spread out over several locations, a written survey may be preferable over an in-person workshop. However, a workshop could be more valuable for front-line workers to ensure they feel like their concerns are being heard.

It's vitally important that whatever methods you use are tailored to your organization...even if it takes a few times before finding the right mix. If it seems like things aren't working like they should, don't abandon the process altogether, but rather see it as an opportunity for improvement.

- **Relying on a single identification method**

Only using one method for your risk identification is fraught with all kinds of consequences. The first problem, explained above, is that a method you use for middle managers will not work so well for executives, and vice versa.

In addition to considering your participants, a combination of risk identification methods is important for producing a more comprehensive list of risks. A participant may include something on a survey that they would not bring up in a brainstorming session. Remember that the goal of the risk identification process is to try and understand all possible scenarios that can affect the company and the achievement of its objectives.

- **Thinking risk identification is a one-and-done activity**

Many organizations, especially smaller ones without a dedicated risk management staff, simply look at risks one time and then ignore the list until something critical comes up. While larger organizations usually conduct a formal risk identification review annually or twice a year, it's important to remember that risks are always changing...so you should always be on the lookout.

Part of the goal of having an enterprise risk program is to get everyone in your organization to be thinking about risks in their day-to-day activities. Not only are risks being identified and steps being taken to eliminate or mitigate them, you are building a company culture that takes the issue of risk management seriously.

The risk identification process can be a little rocky, especially when you're first starting out. It will take time to iron out the right approach for your

organization and refine it so it runs as smooth as possible. **Mistakes are inevitable.**

However, keeping these common missteps in mind during the process can ensure it not only goes as smoothly as possible, but that it also yields a comprehensive, actionable list to carry forward into the next steps of the risk management process.

---

## CHAPTER 2: AT A GLANCE

Although risk identification and risk management involve a lot of trial and error, there are certain missteps that can lead to disastrous results, such as the loss of executive support, loss of engagement from the company, and more.

These mistakes can include:

- Being reactive to a problem
- Not using a methodical approach to identifying risks
- Identifying a risk without understanding scope
- Relying on a single risk identification method
- Thinking risk identification is a one-and-done activity

While mistakes are inevitable, keeping these missteps in mind can help ensure things go as smoothly as possible and that you end up with a comprehensive, actionable list of risks.

# CHAPTER 3: FIVE RISK IDENTIFICATION METHODS AND CHOOSING THE RIGHT ONE

Before selecting your risk identification methods, I strongly recommend taking 3 prep steps to avoid some of the missteps discussed in Chapter 2.

## PREP STEP 1: ESTABLISH THE CONTEXT

As Peter Cockcroft explains, **“establishing the context” is an essential task in preparing for a smooth and ultimately valuable risk identification process.**

The “context” of your effort is simply the focal point: what are you evaluating risks to? As explained back in Chapter 1, your focal point can be something at the highest levels of the company like strategic planning, or it can focus on a one-time project, a process (i.e. payroll, purchasing) or a business function.

The ISO 31000 framework defines this step as:

“By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and the risk criteria for the remaining process.”

## PREP STEP 2: DETERMINE THE APPROACH

A top-down approach is applicable to board members, top executives and high-level directors and usually involves strategy and the “bigger picture” of the company.

A bottom-up approach is very detailed, applies to projects, functions or processes and lets executives know what topics concern front-line employees.

Once you have identified the focal point (context), determine whether a top-down or bottom-up approach is best.

As the name implies, a top-down approach is applicable to board members, top executives and high-level directors and usually involves strategy and the “bigger picture” of the company. Information gained from top-down risk identification can be filtered down to middle managers and workers as appropriate. Therefore, if you will be identifying risks to the company achieving its overall objectives and will be working with executives, you will want to use a top-down approach.

A bottom-up approach on the other hand applies to projects, functions or processes and goes into a lot of detail. Participants in bottom-up risk identification will include middle



managers and front-line workers who will report a detailed list of risks up the chain to their respective business unit leaders who then determine what executives need to know.

Also, a bottom-up approach is useful for helping company leadership understand what front-line workers are really concerned about, while helping employees feel like their voices are being heard.

### PREP STEP 3: ESTABLISH INTERNAL AND EXTERNAL FACTORS

A big part of getting the right risks identified, regardless of the method, is establishing the external and internal factors for both the company and context. These factors define the environment in which the company operates; understanding them is important for prompting accurate risk identification among participants.

Examples of external and internal factors can include:

- **External**: Social, cultural, political, regulatory, technological, economical (local, regional, national, international), and competition.
- **Internal**: Organizational culture, governance, policies, capabilities, standards, objectives, and strategies.

Once you have established the context, determined the right approach, and identified internal and external factors, you are ready to select a method.

# THE RISK IDENTIFICATION METHODS

Now that we've covered what risk identification is, how it can be used, and mistakes commonly made during the process, we're ready to discuss various methods organizations can use for identifying risks.

- **Workshops (Top-Down)**

**Best Use:** Identifying enterprise-level risks using a relatively small group of executives or directors.

Facilitated workshops are considered by thought leaders and researchers to be highly effective. It is the right choice to consider if the context of the inquiry is top risks to the whole enterprise, not risks at the functional or business level. This top-down approach is suitable for a small-to-medium group of board members, top-level executives, and senior directors.

Workshops can help participants identify different types of risks (new, evolving, and emerging), discover connections between risks, and ensure the right people are responsible for them (i.e. risk owners). Workshops are also valuable in establishing a risk culture at the enterprise.

You, the risk manager, will be responsible for organizing and facilitating the workshop. So be sure you think through how you want to capture information being provided by participants (have them write down post-it notes or does someone else take notes?), get discussion going and on topic, and how you will handle any potential heated discussions. Also, don't be overly ambitious with your allotted time – if you think a discussion will take 15 minutes, it will likely take 30 minutes. Be prepared to adapt

your plan to the circumstances, but have the tools to keep the conversation moving.

One of the biggest challenges of facilitated workshops is determining which executives should be involved. In some organizations, executives work in silos, leaving them unaware of the organization's daily operations. While these individuals would be great subject matter experts for their areas, they may not be able to identify high-level risks to the organization.

Additional challenges include clarifying goals of the workshop, ensuring common risk language and definitions, and scheduling. Synthesizing the comments into a meaningful list of high-level risks can also prove difficult. Also, be sure to share your results with the group to ensure you accurately captured their concerns.

- **Interviews (Top-Down)**

**Best Use:** Identifying major risks to the organization as seen by an executive or manager.

The interview is a one-on-one method for identifying risks where an executive or top-level business manager provides his input on major risks facing the enterprise. As the company refines its methods, additional individuals can be interviewed.

As a risk identification method, interviews can uncover more delicate risks than workshops because the participants feel more comfortable discussing sensitive topics in a private setting. Also, the one-on-one, personalized nature of interviews helps gain vital support for the risk management (ERM) process from the company's top leadership because it provides the executives an opportunity to ask questions in this private setting.

The process usually consists of the executive being interviewed, one risk manager to ask the questions, and another person to transcribe the responses.

Aside from scheduling time with the executive, the biggest challenge with using interviews is interpreting the results, including understanding the concerns and classifying the organizational risks.

You can overcome these challenges with pre-planning. Start the process early and allow time for rescheduling if necessary. Create a list of questions to be used in all the interviews to establish consistency. Then, develop a plan to follow-up with each interviewee to confirm your understanding of their concerns and resolve any miscommunication.

- **Scenario Analysis (Top-Down or Bottom-Up)**

**Best Use:** Identifying high-impact low-probability risks to aid in strategic decision-making.

Scenario analysis can be used as either a top-down or bottom-up approach. This method is especially useful in determining risks for events with a high impact but a low probability of occurring—including those that could prove fatal to the organization.

The scenario analysis method should be considered when strategic planning is underway, if leadership is seeking a deeper understanding of risks, managers are seeking more support for mitigating risks, or the organization is undergoing a major change and wants to understand its potential impact.

The process of scenario analysis involves asking a lot of “what if” questions. When done properly, it can help the organization discover new risks in murky situations or improve mitigation measures for currently known risks. It helps spark debate and challenges participants to think about factors they would not otherwise consider. The cross-functional nature of scenario analysis also helps to identify interdependencies, blind spots, or biases.

On the flip side, scenario analysis workshops can be demanding. In addition to scheduling constraints, participants may take issue with the challenging nature of the questions. It can also be difficult for risk managers to prepare for this type of workshop because the “what if” questions are based on the participants’ responses. (For example, “You stated that if you had damage to your building, you would have your employees work remotely. What if their laptops are left in the damaged building, leaving them with no technology to support that strategy”?) The key is to remain calm and flexible and to focus on the high-impact risks.

- **Surveys (Bottom-Up)**

**Best Use:** Identifying multiple risks across an organization.

A risk identification survey can be sent out to a large number of individuals within the company. While this approach is typically focused on the context of business units or operations involving middle managers and their support staff, executive leadership may issue corporate-wide surveys to identify underlying risks to the organization. Surveys can also be the best method if workshops and interviews are impractical, such as when personnel are dispersed in different locations.

Many organizations will take an open-ended route with their surveys by asking employees to identify, in their own words, what they believe are the

top risks. Participants are then asked to rate how well management is responding to those risks.

One of the benefits of using a survey is to give lower-level employees the opportunity to identify risks without fear of reprisal. This method also helps management identify new risks and gauge the impact of those risks from the staff's perspective.

The primary challenge, though, is how to handle such a large volume of information. Before releasing the survey, ensure you have the processes and tools in place to capture, evaluate, and report on the responses.

Specifically, this process should outline how to determine which risks are enterprise-wide and how that information will be shared with executives.

- **Root Cause Analysis (Bottom-Up)**

**Best Use:** Understanding the root cause for known issues and using that information to identify risks to the organization.

Root cause analysis is unique among the risk identification methods. Instead of asking about potential risks, it starts with a known problem and works back to the primary cause. Once the chain of events is understood, it can be examined more closely.

At a basic level, anyone within the organization can determine the root cause of a problem by continuing to ask why something is happening, (e.g. why projects aren't being completed on time). However, if the risk manager facilitates this discussion, he can listen for any dependencies or consequences to known strategic, operational or financial objectives, uncover opportunities to create additional value, and identify new risks.

Root cause analysis is also highly useful since it primarily involves employees and managers at the operational level who can unearth additional and emerging risks that may not be apparent to other areas of the organization.

Since this analysis often dives deep into processes, this method is too detailed to be used with executives.

Before starting a discussion on root cause analysis, do your homework. The more you understand about the processes you will be discussing, the more efficient and beneficial the meeting will be. You may also want to reach out to various departments (especially the project managers) to ensure that results of their root cause analyses are made available to you.

---

Now that you've seen the top risk identification methods, determine which one is right for the situation by establishing the focal point of the inquiry, the internal and external factors that affect it, and the individuals you need to involve (i.e. executives or front-line staff).

For example, if you are working with executives to identify strategic risks at a high-level, a root cause analysis is not going to work. On the flip side, an interview with an executive is not the right way to go if you are trying to understand why employees are not getting paid on time.

Also, don't feel restricted to use only one method. If you perform a workshop with executives, you may want to follow-up with one-on-one interviews to confirm the results, uncover more, and request updates. Employee surveys can also help reinforce executives' assumptions.

Remember, an organization should NOT rely on a single method for risk identification...and neither should you!

As explained in Chapter 2, using **a combination of risk identification methods is critical for ensuring the organization ends up with the most comprehensive list of risks possible.**

---

## CHAPTER 3: AT A GLANCE

Finding the right risk identification involves more than just pulling one out of a hat. The context of the inquiry and any internal and external factors must be understood first.

Determine the approach (top-down or bottom-up) based on who will be involved.

Top-down risk identification methods include workshops, interviews, and scenario analysis.

Bottom-up risk identification methods include scenario analysis, surveys, and root cause analysis.

Using a combination of methods ensures a more comprehensive list of risks.



## CHAPTER 4: CONCLUSION AND FINAL THOUGHTS

I agree with other ERM thought leaders and professionals that risk identification is the essential foundation for the entire risk management process. That's why mistakes at this point can lead to a host of consequences, including wasting time and resources and limiting the value of ERM.

I say that not to frustrate you, but to encourage you! Successful ERM programs are born of trial and error, not by copying other companies or applying a cookie-cutter approach to everything. When you determine that a method doesn't work for your organization, or in a specific circumstance, write it down. Reflect on my lessons learned to ensure you don't make the same mistakes again. If appropriate, give your apologies and explain (briefly) that your process is still maturing.

Over time, you'll develop risk identification processes that fit your organization and the content being reviewed. It's important to be methodical and consistent in using those processes and capturing risk information from your efforts.

Just as important, however, is the need to be adaptable. Personnel changes, leadership changes, external events, and more can instantly affect how an organization should approach risk identification. For example, a new CFO may be too overwhelmed to commit to a lengthy interview, or a financial crisis may present new risks as well as opportunities. Your ability to be adaptable will ensure the risk management process does not break down completely. Additionally, your willingness to adapt to the needs of the

organization will be appreciated by executives, which will help to build support for the program.

I trust you have enjoyed this e-book and will find it useful for understanding common mistakes, popular risk identification methods and how to choose the right one. For more on risk identification and the enterprise risk management process in general, visit my website at [www.ERMInsightsByCarol.com](http://www.ERMInsightsByCarol.com).

## EXTERNAL SOURCES

- [Putting Risk into \(your\) Context](#); Peter Cockcroft, Feb. 2016.
- [Enterprise Risk Management – Tools and Techniques for Effective Implementation](#); presented by Institute of Management Accountants; authored by William G. Shenkir, Ph.D., CPA and Paul L. Walker, Ph.D. and CPA, 2007.
- [Enterprise Risk Management](#); Dr. Olaf Passenheim, 2010.
- [The Many Ways to Identify Risks - RiskAcumen.com](#); Dr. Paul L. Walker, Dec. 2016.
- [Root Cause Analysis Gets to the Heart of Risk Management](#) – Owen-Dunn Insurance Services; Jun. 2014.
- [Enterprise Risk Management: Frameworks, Elements and Integration](#); presented by Institute of Management Accountants; authored by William G. Shenkir, Ph.D., CPA and Paul L. Walker, Ph.D., CPA, 2011.
- [World-Class Risk Management](#); Norman Marks, 2015.

## BONUS: METHODS TO IDENTIFY RISKS QUICK REFERENCE GUIDE

I trust my comprehensive guide provides you with helpful insights on choosing the best risk identification method to match your organizational or project goals.

However, referring back to this guide can be cumbersome when you are trying to quickly pinpoint the right method for a particular situation.

With this in mind, I want to extend an additional offer: a quick reference guide you can print or keep on your mobile device for quick reference.

### **You can obtain this handy quick reference table one of two ways:**

1. LinkedIn – [Click Here](#)
2. Twitter – [Click Here](#)

For further assistance with risk identification for your organization, or enterprise risk management in general, please contact me today.

Carol Williams, CRM

[Carol@ERMInsightsbyCarol.com](mailto:Carol@ERMInsightsbyCarol.com)

850.212.6693

