Enterprise Risk Management Concepts and Strategy for Small and Medium-Sized Companies

ERM4/23/V1

201 N. King of Prussia Road
Suite 370
Radnor, PA 19087
P : (610) 688 4477
F : (610) 688 3977
info@surgent.com
surgentcpe.com

FIRM SOLUTIONS

Choose Surgent to be your firm's trusted resource for essential education.

Whether you need convenient online CPE programs or tailored in-house programs, we offer a full range of solutions to fit your needs.

ASK FOR A DEMO
of our Firm Portal!

Our **Versatile Educational Options** Include:

ON-SITE TRAINING

Utilize Surgent's renowned instructors and top-rated course materials. See for yourself why our Ethics, Tax Reform, A&A and Yellow Book courses have become the trusted source for CPE in the Accounting industry.

FLEXIBLE FIRM-WIDE ACCESS

Get 12 months of firm-wide access to any Surgent live webinar, self-study PDF, or on-demand webcast—with no need to buy seats or licenses. Available in increments starting with 100 CPE hours.

PRIVATE WEBINARS

Let us schedule private showings of our webinars on dates that are convenient for you. Choose from our extensive catalog of over 10,000 CPE Credits or from one of our 50+ brand new courses.

FIRM PORTAL

Surgent's Firm Portal is the latest CPE innovation, allowing you to track and manage continuing professional education for all users in your organization quickly and easily. Create a positive impact across your organization, knowing you have a solid handle on your firm's training and CPE compliance.

CONTENT LICENSING

Use Surgent's cutting-edge content and PowerPoint presentations with your own instructors.

Contact the **Firm Solutions Team** to Learn More:

Kris Moretti
morettik@surgent.com
610.994.9296

Joe Rastatter
rastatterj@surgent.com
610.994.9618

Surgent cpe
EDUCATION FOR PROS

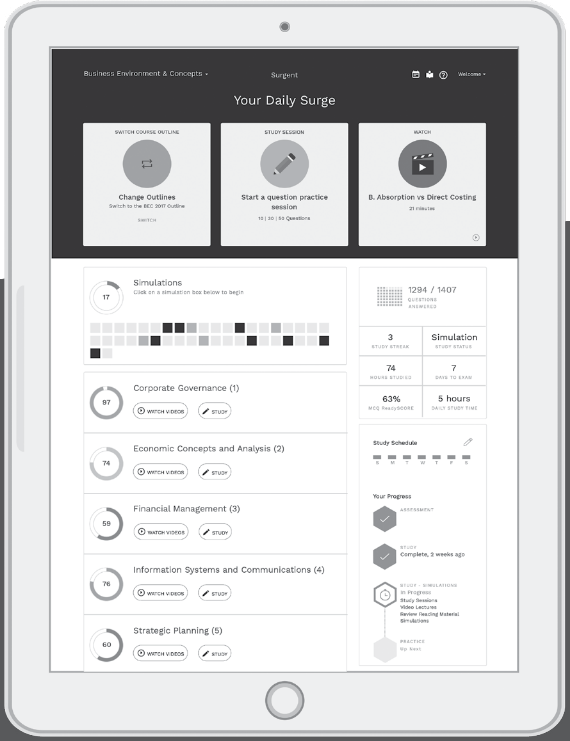
Surgent EXAMreview

Industry-leading exam review courses

THAT HELP CANDIDATES ***PASS FASTER***

Surgent’s AI-powered software personalizes study plans for each student, targeting knowledge gaps and optimizing those plans in real-time.

This award-winning approach has been shown to save candidates **hundreds of hours** in study time.



Your Daily Surge

Change Outlines
Switch to the BEC 2017 Outline

Start a question practice session
10 | 30 | 50 Questions

B. Absorption vs Direct Costing
21 minutes

Simulations
Click on a simulation box below to begin

1294 / 1407 QUESTIONS ANSWERED

3 STUDY STREAK | Simulation STUDY STATUS
74 HOURS STUDIED | 7 DAYS TO EXAM
63% MCQ ReadySCORE | 5 hours DAILY STUDY TIME

Corporate Governance (1) — 97
Economic Concepts and Analysis (2) — 74
Financial Management (3) — 59
Information Systems and Communications (4) — 76
Strategic Planning (5) — 60

Your Progress
ASSESSMENT
STUDY — Complete, 2 weeks ago
STUDY - SIMULATIONS — In Progress: Study Sessions, Video Lectures, Review Reading Material, Simulations
PRACTICE — Up Next

How A.S.A.P. Technology™ Works:

ASSESSMENT

- ✓ Students complete a series of quizzes with content from all exam categories.
- ✓ A.S.A.P. Technology analyzes results alongside real exam scoring and calculates a baseline ReadySCORE™– a highly accurate estimate of what they’d score on their exam if they sat that day.
- ✓ Students receive a Diagnostic Report, detailing their starting strengths and weaknesses and estimates needed study hours.

STUDY

- ✓ Using assessment results, our course builds a personalized plan to close identified knowledge gaps.
- ✓ Real-time algorithms continue to optimize study plans based on progress.
- ✓ Students can see their ReadySCORE improve as they study.

REVIEW

- ✓ Unlimited practice exams – designed to match the actual exam—ensure they will be totally ready come exam day.
- ✓ Once students achieve a passing ReadySCORE, they know they’re ready to pass.

A.S.A.P. TECHNOLOGY

helps you pass the

CPA Exam | CMA Exam

EA Exam | CIA Exam

CISA Exam

Benefits for Associates and Firms:

- ✓ A.S.A.P. Technology gets candidates CPA Exam-ready in just 58 hours, on average, and drives pass rates nearly 40 points higher than the national average.
- ✓ Staff can more easily balance full-time work and study, thanks to a study program that takes into account what they already know.
- ✓ Surgent’s course content complements the adaptive model—and today’s learners—with video lectures and clear answer explanations that teach specific concepts.

Questions? Contact our Firm Solutions Team at **877.721.3565** or **info@surgent.com**

Surgent.com/exam-prep

Table of Contents

This product is intended to serve solely as an aid in continuing professional education. Due to the constantly changing nature of the subject of the materials, this product is not appropriate to serve as the sole resource for any tax and accounting opinion or return position, and must be supplemented for such purposes with other current authoritative materials. The information in this manual has been carefully compiled from sources believed to be reliable, but its accuracy is not guaranteed. In addition, Surgent McCoy CPE, LLC, its authors, and instructors are not engaged in rendering legal, accounting, or other professional services and will not be held liable for any actions or suits based on this manual or comments made during any presentation. If legal advice or other expert assistance is required, seek the services of a competent professional.

Revised April 2023

Introduction

Introduction

Learning Objectives

Upon completing this chapter, the reader will be able to:

- Understand the concept of this course;
- Know the definition of risk management; and
- Understand old and new types of risk management.

I. Concept of the course -- Not for the multi-national

Risk management is a concept extremely familiar to finance professionals in large organizations, and often somewhat familiar to finance professionals in all the rest of the types of organizations. Multi-national organizations, especially finance organizations, have been dealing with risk management for decades; however, often the public accountant advising the small and medium sized enterprise (SME) understands risk, but does not regularly advise how it is to be best managed. This program is specifically designed to remedy that issue.

Because the multi-national, financial, and healthcare organizations have refined the field, especially after the financial breakdown of 2008, most of the literature has been directed toward this group. These organizations have dedicated risk managers and enjoy sophisticated software to aid them in their tasks. They regularly subscribe to publications and attend conferences dedicated to risk management. In fact, they are experts in the field.

A. Designed for the SME

Unfortunately, often finance professionals who do not fall into the multi-national category understand the concept of risk but have not had either the training or experience in moving through the steps to effectively assess and mitigate the risks of the smaller organization. This program is for those finance professionals. Public accountants dealing with and advising smaller organizations have a great need to know both how to motivate and how to generate a conversation about risk with management. In turn, industry accountants of those SMEs need to be up to date on how risk affects the organization and how it can be mitigated, managed, and/or reduced.

It is interesting to note a huge difference between the SME and the larger organization. In the former, the senior (and often the only) finance professional in the organization is by default the risk manager. On the other hand, in the large, financial, and healthcare organization there is usually a dedicated person or department dealing with risk management.

B. Structure, not details

Every organization has risks. The car dealer’s risks often revolve around marketing, the economy, controlling margins, and financing; whereas the non-profit performing arts center has risks dealing with the popularity of shows and the ability to raise donations. While this program will use a lot of specific examples of risk management, it will not go into great detail on mitigating risks in specific industries. Instead, we will attempt to show structured ways that any organization of any industry can assess, mitigate, insure, and better control the various types of risks. For example, cyber risk is a huge field, and would be well deserving of either one or more complete programs. However, in this case we will devote a single chapter to the risk in the second part of the program. Why such brief attention to such an important topic? Simple—our design is to explore a system to manage risk that can be applied to any type of risk or any type of organization. Then, using that system, you the finance professional, can apply it to your organization with your specific risks.

1. Types of risks

We will discuss many, but certainly not all, types of risks that an organization can incur. Some of the risks may be measurable in an objective way, and others will be almost impossible to measure. In the second part of the program we will drill down into specific risks facing the organization; however, in the first part we will primarily discuss building a structure and plan to better manage any risk. In addition, we will spend significant time discussing different types of strategy risks that are often totally missed in other risk management discussions.

In my opinion, this is largely due to a bias in the risk management community. Please understand that I am not a professional risk manager, and thus I approach the subject from the standpoint of a finance professional and senior management. Professional risk managers love to approach risk as a measurable and manageable discipline; however, many of the most important risks of an organization are highly conceptual and virtually impossible to measure. I was once reading an article saying that these types of risk should not be considered in risk management. I was appalled at this statement, since, in my opinion, they represent some of the largest risks that the organization can face. By ignoring them because they can't be measured is to pretend that they don't exist. Obviously, that strategy can prove fatal to the organization that experiences an example of that risk.

A great example of this occurrence is the retail bookstore industry. If you were the finance professional with a bookstore, would you have alerted management to the risk that someone like Jeff Bezos would completely disrupt your industry and force you to re-think your business model. Yet, that happened and a lot off bookstores went out of business because they were unable to compete against Amazon's efficiencies and innovation. Protecting the company against that kind of risk is difficult, but possible. But first the risk must be recognized, evaluated, and a plan put in place to mitigate its eventuality.

II. Definition of risk management

Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Obviously, that's a handful, but explains what this program is all about. All business is at risk and entrepreneurs quickly know the risks they take just by being in business. However, in most cases those business owners are too busy thinking about the business to direct their attention specifically to a better understanding of the risks. That's where the finance professional comes in. It is our job to recognize and evaluate those risks and establish a program to lessen or mitigate them whenever possible. In this way, we serve the owners.

A. Old and new thinking about risk management

Several years ago, risk management was usually another, and somewhat more sophisticated way of describing insurance. The discipline was mostly discussing insurable risks and determining the right mix of deductibles and insurance rates for the benefit of the company.

B. ERM

Today, things are very different. Our objective is to look at the entire company. I like the following definition of enterprise risk management that I found on Google:

> "Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings."

As you can see from this definition, the discipline is far more than managing insurance. Most importantly, it is training the company to view all operations from a risk perspective. We will look at strategy risk, operational risk, financial risk, marketing risk, reputation risk, cyber risk, as well as numerous other kinds of risk. All business represents risk, and the organization must be managed with risk in mind at all times.

That being said; we don't want to develop a risk-averse enterprise. While business represents risk, it also represents gain. The key is to be able, as best as possible, to measure and attempt to properly equate risk and gain.

III. Changes from Covid-19

Obviously, something huge has recently occurred in our business world that seemed to come out of nowhere and has had probably the greatest effect that most of us have ever seen. Could we have anticipated that occurrence? Could we have included it among our identified risks to be mitigated? What could we have done better or what should we change to do better in the future?

The opinions are many as to these and similar questions. Probably the greatest lesson is that we should constantly work toward being more nimble organizations so that we are in a better position to react to unexpected changes. No matter how good our risk-management program might be, we will miss some, but we still have to react. Throughout this course, we will attempt to comment on changes which should be made from what we have learned from this experience.

A. Black swan or gray rhino?

Black Swans: Nassim Taleb defined "Black Swan" events as rare and hidden, highly improbable, and unforeseeable. We cannot develop a response strategy before they occur. 9/11 was one such event.

Gray Rhinos: Michele Wucker identified "Gray Rhino" as an obvious, highly probable threat that can be seen in advance and thus prepared for, but which is ignored or dismissed.

Many people see the recent pandemic as a black swan, but it is not. Dr. Larry Brilliant, an eminent epidemiologist, has been a long-term voice on the risk. He was awarded the esteemed Ted Prize for his 2006 Ted Talk titled, "My wish: Help me stop pandemics." Viral infections and the spread of disease are geopolitical risks in the category of gray rhinos. We saw the pandemic possibility. We dismissed it and failed to cooperate with global efforts to respond to it.

Overview of ERM

Overview of ERM

Learning Objectives

Upon completing this chapter, the reader will be able to:

- Understand the potential problems with enterprise risk management;
- Know what is needed for good risk management;
- Know the three main parts to risk management; and
- See why risk management must cover both positive and negative risks.

I. Monitor centrally – Manage de-centrally

As said in the introduction, ERM represents the discipline of risk management on an organizationally wide basis. Rather than being seen as a way to control insurance costs, or the costs of any specific aspect of risk, ERM attempts to view the organization in its entirety recognizing that all aspects of risks will eventually affect the whole organization.

That being said, however, we need to remember who will best be able to manage that risk. To answer that question, ask yourself some simple questions:

Q. Who is the best person to manage marketing risk?
A. The marketing manager and marketing department.

Q. Who is the best person to manage operations risks?
A. The operations manager and the individual parts of the operating departments.

Q. Who is the best person to manage strategy risks?
A. The senior management team.

The answers to all of these, and similar questions, point to the departments themselves being the ones who truly understand the details of the risks they face. Consequently, they are also the ones that are in the best position to quantify, evaluate, and mitigate those risks. Risk management should be seen as a decentralized operation and not a top-down discipline.

However, the total responsibility should not be left to the various departments. In fact, in most organizations one person must have the ultimate responsibility for risk management on an organizational basis. The reason is simple. One person should be in a position to assess the organization in its entirety. He or she must see the whole picture and be in a position to see how a higher risk in one area might offset a lower risk in another area. The individual managers of the separate areas are the most knowledgeable and skilled to manage the risks in their area; however, will generally have less knowledge in another area. The overall risk manager does not have to have specific knowledge in either area but must know how to balance out the risk in the organization.

II. Control issues

As we look at the organization, we should attempt to divide areas into ones where we have control and others where we have little control. For example, in pricing, we have total control of the price we charge for our product or service. Some in the organization may say that we have to follow the market, and that may be true, but the end result is that we make the choice of the price we will charge. However, the price we charge certainly does enter into the risk of the organization.

Weather, on the other hand, is totally out of our control. The fact that a tornado may hit our midwestern plant or a hurricane will demolish our warehouse in Florida is far beyond our control. Yes, we do have control on where we locate our plants and warehouses, but the weather is beyond our control.

In reality, most of our risks are partially under our control. Having a worker "go postal" and harming other employees is most obviously beyond our control; however, actually we do have some control over it. Our culture becomes a huge sum of many of our policies, rules, our hiring, and motivation policies, and most importantly the leadership skills of our managers. So, through those things, we actually do have some control over the environment in which our employees work.

A. Risk strategy

The key strategy when looking at the control issues is simple, but not necessarily easy. On those things about which we have control, maximize those areas, and control them well. Act on things we control, and act on them well.

With areas where we have no control, we should try and minimize those items. For example, we might consider locating that plant in the rocky mountain west where violent storms are much more rare. Or we can, and probably should, insure the plant against storms. Those are two obvious ways of minimizing or mitigating the risks of an event over which we have no control.

About the areas where we have some control, we must first recognize the control we do have. For example, many people would say that we have no control over an employee going "postal." But, as was mentioned, we do have control over our culture, and therefore, partial control about our employees' behaviors. That's why we need to bring risk management into the discussion of hiring and management policies.

III. Problems with ERM

Wow! I thought that this program was all about risk management and especially enterprise risk management. Now, do you want to talk about problems with it? Yes, because if we don't recognize its weaknesses, we will not know how to avoid the problems it could cause.

A. ERM will not eliminate risks

This should be obvious, but often isn't. We have seen many organizations develop an ERM program and by doing so believe that they have essentially eliminated the risk from the organization. This is not the case. The program may have reduced many of the risks and did a better job of quantifying the nature of the risks, but every organization has its own set of risks which must be recognized. The recent pandemic has certainly proven this fact. Despite our program, the pandemic happened, and most organizations were not prepared for it. The gap in their ERM programs was exposed.

B. Little agreement of what ERM programs should look like

Unfortunately, lots of bureaucracy has entered into the risk management industry mainly because it is often the subject of government regulation. Consequently, governments, corporate regulators, and even world-wide standards often differ on what the "ideal" ERM program should resemble. This can be a major problem for the large highly regulated organization, but often much less of a problem for the SME. Fortunately, in most cases our organization can design an effective ERM program based on these, or other similar, materials and with the advice and council of our stakeholders.

C. What we know does not work

1. Ad hoc and unsystematic risk management

Unfortunately, a huge amount of SMEs have this problem. It is often evidenced by such statements as, “We know the risks in our business, and we don’t need an outsider telling us how to manage them.” Yes, owners and managers of small businesses often do understand the risks that their organizations face, but in most cases, they have not developed an organized system to evaluate, measure, and mitigate those risks. Consequently, in some cases things work out just fine, and in others, suddenly the wheels fall off and the organization goes out of business. This problem often happens when management is highly experienced in the particular field and has been successful. Statements like, “I’ve always done it this way and it’s always worked,” are often heard. For the finance professional looking to structure an organized ERM program, this type of thinking will present a significant problem.

2. Thinking that insurance equals risk management

This problem is very prevalent in organizations where risk management is not really understood. Often insurance experts use the title, “risk manager,” but often have little perspective about the nature of things like strategy, reputation, or other non-insurable risks. Insurance is important, but only one part of risk management.

3. Relying on regulations and regulators

A good ERM program should be pro-active rather than re-active. We should always be on top of what’s happening in our area of expertise and refining and adopting our ERM program to the latest developments. For example, in the last few years the banking industry has unveiled systems allowing their customers to deposit checks directly into their computers and to the banks. Unfortunately, this operation, while efficient, opens up the organization to new risks. Ask yourself a simple question, do you think that the regulations and regulators are up to speed with these new risks? I would guess no, and therefore it is the responsibility of the organization’s ERM system to adapt to the changes in risk. Thinking that the government or some regulator will tell me how to do something is a great fallacy that must be avoided.

4. Relying on perspective-based controls rather than performance-based controls

Perspective-based controls are checking off the box that says that, “we are doing that.” These controls are often used in audits and have a person attest that certain things are being done. Unfortunately, checking the box may have nothing to do with determining if the control is effective. Well known consultant Peter Drucker coined the concept that good management is doing things right. Good leadership is doing the right things. Performance-based controls represent controls that have been based on performance and are proven to actually prevent the wrong things from occurring. Unfortunately, many larger organizations fall into this trap where they follow the rules well, but unfortunately, they don’t have the correct policies. As we go further into this whole ERM subject, we will look more into the difference between rules and policies, and how they affect risk management in the organization.

5. Following industry norms

You might properly call this the “lemming” effect – doing what everyone else is doing. I find that these problems are most apt to happen when many management people attend and receive their training through trade conferences and similar events. We brush up against and learn from others in the field to the point that everyone is doing the same thing. We follow, “best practices.” I’m not saying that the concept of best practices is necessarily bad, but I’m asking you to ask a simple question. How does a practice become a “best practice”? The answer is usually because it has been proven to work over an amount of time. Now ask yourself another question. If the organization operates on best practices, will it be changing as fast as the world around it? The answer is obviously not; and that, in itself, presents a huge problem and a significant risk. We will deal with this more when discussing strategy risk.

6. Hidden agendas

Unfortunately, people in the organization often have their own agendas that they are pursuing without telling others. In all cases, these agendas are selfish and usually hurt any effort to establish a successful ERM program.

a. **CYA** -- Unfortunately, people in some organizations have specific agendas to avoid taking any risk. Often this is the product of a very bureaucratic risk-averse culture where people are highly criticized for making mistakes, but seldom praised for doing the right thing. Consequently, they will often do anything they can to avoid being caught making a mistake or being blamed for mistakes. This behavior harms a balanced ERM program.

b. **Compliance with rules** -- While it’s obvious that organizations need to be compliant with rules and regulations; often, however, the organizations can be totally oriented in that direction without seeing risks in other areas. These organizations will be able to say that they followed all of the rules, but they ignored a potential risk that wasn’t mentioned in the rules. As an example of this kind of problem, I love to site the example from an old Broadway play later made into a movie, “Please Don’t Eat the Daisies.” The crux of the plot was that a mother and father took a short trip and left the older child in charge of the younger. They left a very long list of all of the dos and do-nots. The younger child ate the daisies in the table centerpiece and got sick. When the parents came home, the older boy proudly said that he had carefully followed the list of rules, and nowhere on the list was the rule not to eat the daisies.

c. **Get money for pet project** -- In some organizations, silos develop where managers are highly protective of their areas of responsibility. Consequently, they will be less than candid when it comes time to accurately assess the risks associated with their projects. All of their projects have low risks and high rewards.

d. **Validate or support someone’s preexisting opinion** -- Psychologists often talk about “confirmation bias,” which is a person’s tendency to search for, interpret, favor, and recall information in a way that confirms one’s preexisting beliefs or opinions. As we develop an effective ERM program, we must be cautious that research is as free as possible from this problem.

IV. Needed for good risk management

In order to achieve good risk management, employees throughout the organization MUST do the following.

A. Understand the risk management system

Risk management is relatively simple, but many don't understand it. For years, risk management has been seen as managing insurance policies, and most employees have figured the experts in the field will handle the issues. With ERM, all employees should understand why:

1. Risk is at the heart of any free-enterprise organization;
2. Risk isn't bad;
3. Risk can be managed for improved results of the organization; and
4. Risk management is the responsibility of every employee in the organization.

B. Trust the risk management system

A key part of the system design is to establish it as an organization-wide program where everyone has a part in its design and implementation. If the program is "owned" by the finance or risk management department, many employees will not see it as their responsibility and rather the responsibility of the experts. For that reason, as we will see in future chapters, the program must involve all departments and at all levels. For example, if the organization has a fleet of vehicles, how they are driven and maintained obviously has a lot to do with risk. Management can recognize that fact, but if the drivers don't participate in the management, risks and costs will increase.

Remember that the idea of an ERM program is to establish and monitor the program centrally, but risks must be managed de-centrally where people understand the risks best.

V. Three main parts of a risk management program

While the subject can be sliced and diced in many different ways, the three main parts of an ERM program are to identify the risks, attempt to quantify them, and set up a strategy to maximize the gains and minimize the losses.

A. Identify

In this phase, we identify the risks. While we will end up identifying for the entire organization, actually the process will be for the people in a particular area who will identify the risk for that area. The finance department will identify the risks for the finance department, the marketing department will identify marketing risks, and the operations people will identify operating risks.

1. Too many risks identified

As we said earlier, there are obviously a huge amount of risks in any area. Consequently, a huge problem develops when too many risks are identified and the whole ERM program seems daunting and not worth the effort. On the other hand, the way to fix this problem is to layer the efforts in such a way that any one group only is concerned with that group's risks. For example, there are a great number of risks in the finance department, but if the collection team was the one to identify their risks, then the task is manageable.

2. Over-estimation of risks

Some organizations who go through this process will identify too many risks to the point that the organization becomes a risk-averse organization. When this happens, the final result is an unrealistic process that is no longer manageable.

B. Evaluate

Because we need to avoid the above-mentioned problems, we must somehow quantify the risks in such a way that we know better if they even need our attention and how we might manage them.

1. Over what period of time

As we enter this process, we have to establish a benchmark dealing with time. After all, something might not be an immediate risk, but if we look at the origination over a long period of time, the chance of occurrence increases. In marketing, we might be in a very good competitive position, and therefore the risk that a competitor will undercut our pricing is relatively small. In that case, we might quantify that risk as small. However, over a five-year period of time, and if we don't make changes to be more and more efficient, then the chances that we will be underpriced becomes high. Therefore, an early part of the program is to set a time frame for the ERM program.

Activity:

For your organization, discuss what should be the time frame of a risk management program. Justify your opinion.

2. Often comparing apples and oranges

How do you compare the risk of a tornado hitting your plant to your business model being disrupted through innovation? Both are obviously risks that need your attention, but how do you rank one against another? The answer is to use some kind of model that allows you to put the risks on a grid and quantify two specific aspects of the risk.

a. **Severity of the risk and impact on the organization --** In this case, we will attempt to evaluate how severe this risk would be. For example, a little shoplifting in our retail store selling inexpensive items would probably be classified as not very severe. On the other hand, if we sold high priced diamonds in our store, we would probably rate the shoplifting risk as quite severe.

b. **Likelihood of occurrence --** The other aspect of evaluation would be to attempt to estimate the chances of occurrence. If we look again at the retail store, the likelihood of shoplifting would be high, especially if a lot of customers are in the store at one time. Consequently, we manage that risk based on the value of the merchandise being sold. We probably don't do a whole lot if we are a convenience store, but spend a lot of money and make major efforts to prevent the shoplifting if we are a high-end jewelry store.

In both cases of evaluation, severity and likelihood, we are making subjective judgements; however, we have the duty as the risk manager to establish benchmarks of scoring so that we better measure across departments.

C. Mitigate

Once the risk has been identified and quantified, the task is to develop a strategy either to increase the likelihood of a positive outcome or reduce the likelihood of a negative occurrence.

VI. Both positive and negative

It is important to remember at this point that a good ERM program looks at both the positive aspects of risk (reward) as well as the negative aspects (costs). If we don't, and we only focus on the negative risks, then we will become a risk-averse organization which is usually far less successful. If we look at most of the successful innovative organizations over the past years, we see that they have been willing to take large, but calculated, risks to achieve their goals. Jeff Bezos certainly took risks when he started Amazon, and the organization continues to take risks as it explores such things as drone delivery.

Risk Tolerance and Developing a Plan

Risk Tolerance and Developing a Plan

Learning objectives

Upon completing this chapter, the reader will be able to:

- Understand risk tolerance;
- Know how to develop a risk management plan;
- Understand organizational cultures; and
- Understand how organizational culture affects risk tolerance.

I. Start with a plan

We know that all business involves risk, both positive and negative, but properly managing that risk requires a well-conceived plan. Without it, the business runs the risk of either exceeding its intended risk or failing to take advantage of opportunities due to being unwilling to take appropriate risks. For that reason, we need a plan.

The largest of organizations often have completely evolved plans involving hundreds of pages, thousands of statistics, and hundreds of metrics and graphs. The owner of the small business, on the other hand, will often make a statement such as, “I know that my business is risky, and I understand that risk and I control the amount of risk I want to take.” Since this program is directed to the finance professional of the small or medium size enterprise, it is designed to bring some order and planning to the small business without causing it to become as large and bureaucratic as the largest organization.

II. Appetite and tolerance for risk

A. Risk appetite and risk tolerance

Risk appetite is often defined as, “the amount and type of risk that an organization is prepared to pursue, retain or take in pursuit of its business objectives.” A risk appetite statement is a higher-level statement that broadly considers the levels of risk deemed acceptable to pursue a given reward. A risk tolerance statement is a narrower statement setting the acceptable levels of risk surrounding various, different objectives.

For example, if a company were to say that it didn’t want to accept risks that could result in a significant loss of its revenue base, it would be making a statement about risk appetite. On the other hand, if it were to make a statement that it wouldn’t accept risks that would cause revenue from its top 10 customers to decline more than 10%, it would be making a risk tolerance definition. The former would be more of a macro statement; the later would be more of a micro statement.

B. Residual risk

Often in risk management we will mitigate a risk to lessen its potential impact to the firm. Residual risk is the amount of risk left over after the mitigation. For example, there is a very real risk of fire at a manufacturing plant. Consequently, we will ensure that risk. However, often to save money we will have a deductible or some other aspects of a fire that are not insured. Those would represent residual risk.

C. Risk capacity

This represents an organization’s overall ability to absorb potential losses. This can be measured in terms of cash and cash equivalents to meet liquidity demands and in terms of capital and reserves to cover potential losses. In the largest organizations the capacity is evaluated through regulatory stress tests and similar measurements. In the small business, the measurement is less formal, but needs to be calculated. In addition to capital and liquidity, capacity also includes the organization’s skills, management, tools, and performance track record. For example, the organization with a long track record of profits would have a higher risk capacity than the start-up organization even if both had the same amount of capital and liquidity.

D. Risk profile

The risk profile of an organization is tied directly to its strategy. For example, if a company decided to have a strategy of being a low-cost producer, its risk profile would largely be operational risks involving supply chain, operational efficiency, scale economics, and cost control. On the other hand, if the company were built on the idea of being the high-end and of high-quality, its risk profile would be built more around marketing risk, reputational risks, and innovation risks. In both cases, the companies might be equally risky, but the risk profiles would be totally different.

E. Risk-adjusted return

This provides the business with an economic rationale for determining how much risk it should be willing to accept. Actually, no organization should be willing to take any risk unless it is adequately compensated. For any business transaction, the manager should establish the risk-adjusted price to be charged that provides the proper rate of return for the transaction. Included in the costs of the project would be the risk costs including possible loss, cost of capital, insurance, administrative costs, and any other mitigation costs.

Although all businesses take risks, there is only one opportunity to be compensated for that risk – in the pricing of its goods and services. This is a perfect example why all aspects of the business, including sales and marketing, must be involved in the risk management planning of the organization. If not, risk has a way of not being included in the price.

F. Risk tolerance

This is often seen as a synonym for risk appetite, but it is actually very different. Risk tolerances are the quantitative thresholds that allocate the organization’s risk appetite to specific risk types, business units, or divisions. Risk tolerances are the parameters within which the company, division, department, or business unit will operate within to achieve its risk appetite.

G. Risk appetite statement

Once we have assessed the above aspects of risk, we are ready to actually write out a risk appetite statement. While the purpose of the statement is to assure that everyone in the organization is in agreement with the amount of risk to be taken, it has several other advantages. The risk appetite statements’ other benefits are that it:

1. Develops a common understanding and language about risk at all levels;
2. Produces risk assessments and analytics within the organization; and
3. Promotes awareness and enforces the risk culture within the organization.

III. Developing the risk appetite statement

A. Assess regulatory requirements

In many industries, the regulators will require that the statement meets certain requirements. While this is mostly true of the larger organizations, it can also be true of smaller organizations in certain industries.

B. Communicate the benefits of having a risk management plan and a statement of risk acceptance

It is imperative that this starts at the top. As the senior finance professional, it is important that the risk management activity is not seen as coming from your department. If the top management sees risk management as a necessary evil, then the rest of the organization is far more apt to buy into the process. Your first sales job will be at the company C level suite. Following that, it can be rolled out to the entire organization.

C. Organize a series of meetings with risk owners

The sponsor of the ERM project will organize a series of meetings with executives at all levels throughout the organization. The purpose of the meetings will be to discuss risk tolerance and develop the risk appetite metrics for their organizational units. The purpose of the meetings will be to develop the risk appetite statement including all stakeholders. Included in the discussion will be:

1. **Business strategy** -- The business strategies and objectives of the units.
2. **Performance metrics** -- How those strategies and objectives will be measured.
3. **Risk assessment** -- What are the key risks that will drive the performance of the unit?
4. **Risk Appetite** -- What is the appetite for each of the risk areas?

D. Key roles and responsibilities for the risk appetite statement

1. Board of directors

The board of directors will:

a. Review, challenge, and approve the final statement.
b. Provide risk governance and oversite.
c. Be accountable for overall risk strategy.

2. Executive management

Executive management will:

a. Establish corporate risk strategy.
b. Monitor aggregate risk exposure.
c. Be accountable for completing risk appetite statement.

3. Business units

The business units will:

a. Establish business strategies, metrics, and risk tolerances.
b. Report exceptions to senior management.
c. Be accountable for managing risk.

IV. Risk tolerance and organizational culture

A. Understanding cultures

Over the years much has been said about organizational culture; however, probably no person has expressed and defined cultures better than Irish management consultant and author, Charles Handy. In his book, *Understanding Organizations*, he defines four distinct types of cultures: Power, Role, Team, and Individual.

1. Power culture

Often this is a smaller and more entrepreneurial organization started by a single individual. The owner wields the power in the organization and the management system is very top-down. The owner may have a small team of lieutenants in charge of various aspects of the organization, but they directly report to him/her and there is no question from where the power emanates. This organization tends to move and change quickly because the boss can quickly say that we are changing. When the owner is skillful, the organization is usually very successful when it is small. Because the owner tends to want to control everything, problems can easily develop when the organization grows beyond what a single person can control.

This culture is sometimes called a “club” culture, but it tends to be somewhat “clubby” with those in the club and those who are not. It is important to realize this about this culture, especially for the finance professional. We have seen organizations where the owner has a sales and marketing somewhat higher risk tolerance than does the CFO. When that is the case, the finance professional is seen as someone who is hindering the progress of the organization, and thus not in the club.

2. Role culture

This organizational culture is pretty much the opposite of the power culture. Instead of it being a relatively small organization, this one tends to be large, formal, and highly regulated. Like the power culture, the management system is top-down, but the top represents layers of management rather than a single individual. The operating system of the role culture is rules and regulations, and that is what people trust. There seems to be a rule for almost everything. The culture gets its name since everyone in the organization has a specific role. In fact, job descriptions and salary ranges are narrow, and everyone seems to have his or her own title. Often this is called the bureaucratic culture and is found regularly in highly regulated industries like financial services and healthcare. But it is also often seen in non-profits since they tend to be somewhat board-centered and the board tries to control through rules and regulations.

3. Team culture

This can be any sized company from the largest to the smallest. The big difference between the power and role cultures and the team culture is the direction of the management system. While the first two are top-down, the team culture is more bottom-up. That doesn’t mean that the employees run the show, but it does mean that there is much more empowerment at the lower levels, and management trusts employee teams to make good decisions. Consequently, the control method of the culture is results rather than either rules and regulations or executive decisions of the boss.

4. Individual culture

This pertains to a rather unique organization and it is not nearly as prevalent as are the first three cultures. This organization may be a small professional office where there are no real leaders, but the professionals take turns running the office. The culture gets its name because most of the professionals treat the organization as one of convenience, but really, they operate as individuals within the organization.

B. Cultures and risk

1. Power culture

This culture generally has a high tolerance for risk; however, most of the risk taking is done by the leader of the culture. Since the organization is usually owned by a single individual or very small group, that person is the one who makes the risk decisions, and the decisions are generally made in a “seat of the pants” style. The boss will say something like, “I know business is risk and I’m willing to take it to make a reasonable return.”

One problem of the culture is that the boss often does not recognize some types of risk with which he or she may not be familiar. For example, the boss totally understands marketing and product risk and makes skillful decisions with respect to them. But he or she may not recognize other types of compliance risks. For that reason, it is very important that this type of organization enter into an ERM program where all of the risks are taken into consideration.

2. Role culture

This organization probably already has a sophisticated risk management program; however, the organization may very well suffer from being risk averse. Unfortunately, the role culture can take on a culture where people are not rewarded for successes but are severely punished for making mistakes. Consequently, for the individual, it’s prudent to avoid risk and just keep on moving on ahead. Well known management consultant Peter Drucker defined the difference between management and leadership. He explained management as “doing things right,” but leadership as “doing the right things.” In the role culture we often see people doing things very right, and not taking much risk, but they are not necessarily doing the right things and taking appropriate risks.

Change involves risk, which is the primary reason that this culture is very slow to change. Since people are often unwilling to take the risk, the organization lags behind the change in the real world. In seminars, we often ask a very important question:

Is your organization changing as fast as the world around it?

The follow up question is:

If the answer is no, what will happen to it?

Unfortunately, the answer to that question is that it will cease to exist.

For this reason, it’s important that this organization review its risk tolerance policy and make sure that it’s taking enough risk to change as fast as the real world is.

3. Team culture

Generally, this culture does risk management best for a couple of good reasons. First, since it is more bottom-up than top-down, it uses the system that asks the people closest to the risk to actually manage the risk. Remember what we said earlier, “Monitor centrally, but manage de-centrally.” Since the operating team closest to the risk will be the ones to evaluate and mitigate the risk, they will probably do it better than either of the other two main cultures will do it. Either if the boss manages the risk or if some bureaucratic committee manages it, it will not be done as well as if the people closest to the risk will do the managing.

The other reason why the team culture will probably do a better job with risk management is that the team culture controls itself through results rather than either by rules or executive fiat. Consequently, the team is more apt to balance the cost of the risk or risk mitigation more correctly against the return from the project. For example, often the role culture will not want to take the risk to change and won’t see the real risk of not changing. But the culture sees the risk of changing; consequently, it doesn’t take the risk and change either doesn’t happen or happens too slowly.

4. Individual culture

It’s almost impossible to generalize about the risk tolerance of the individual culture because it can be in so many industries. In many cases, the culture actually tolerates much more risk than expected because the professionals are too busy seeing patients and clients and fail to take the time to actually analyze the risk. On the other hand, other individual culture organizations can become risk averse should they become too bureaucratic.

V. Case studies

Throughout this program we will follow two specific organizations, one a for-profit company and the other a non-profit private school. The purpose of the case studies is to use these fictitious organizations as examples of how to apply what is being discussed in the chapter. In some chapters, we may use both companies as examples, and in other situations we will use one or the other. The primary purpose of using both a non-profit and for-profit is to demonstrate how the ERM system will work equally well for either type of organization. Will the applications be different? Sure. But they will be similar.

It should be noted that in both cases, the organizations are completely fictitious and any resemblances to real organizations are completely coincidental.

A. Case study 1, For-profit organization

Ace Electrical Products is a small importer of tools and related equipment sold primarily into the electrical contracting industry. The company has been in business for 20 years, presently has 19 employees, and enjoys sales of about $32 million with a profit nearing $1 million. Bud Phillips is the CEO and owner of the company, and he has a senior management team of 3 consisting of Susan Smith, CFO, Harold Thomas, COO, and Brad Blake, Chief Marketing Officer.

The company started as an electrical wholesale distributor selling primarily to electrical contractors in a large Midwestern city. Bud was brought up as the son of an electrical contractor, and truly understands the industry. But he really didn’t want to follow in his father’s footsteps and went into distribution. Before the company had become very large, he recognized the opportunity of supplying innovative tools to contractors and having the items sourced from offshore. As he took that turn, he quickly sold the distribution side of the business and concentrated on designing, importing, and selling the tools to other electrical supply wholesalers.

The company now operates on a national basis and sells primarily through three salespersons along with a couple of manufacturer representatives. The firm advertises in the trade publications, has a website, and markets at several industry trade shows across the country.

B. Case study 2, Non-profit private school

Northbridge Academy is a small faith-based K-12 school in a small Midwestern town. It has a staff of 18, of which 14 are teachers and has a total enrollment of about 100 students. In addition, it operates a day care pre-school that usually has about 15 young people.

The state in which the school is located has an interesting tax incentive system that helps private schools. This system allows taxpayers to make a donation to a private school and take the gift as a credit against state income taxes. The tax program has been going for 8 years and the school has been very successful in recruiting taxpayers to make donations to the school as scholarships for the students. As a result of this program, about 70% of the students receive this scholarship help. Annual tuition for the school is approximately $7,000.

The school is run by a headmaster and one other person in administration in addition to a small office staff. The 14 teachers are primarily retired public school teachers and others who are proficient in their subject area. The salary scale of the teachers is well below the public-school level and the fringe benefits are poor; however, the school generally has extremely good teachers since they are dedicated both to the students and their faith.

The school runs with an annual budget of just under $1 million with most of the income coming from tuition and tax credits. They have various fundraisers and receive donations from the community. Donation and fundraiser income amounts to about $150,000. Profitability of the school swings greatly depending on enrollment. Almost all of the expenses are fixed in nature and do not change much with enrollment. Consequently, when enrollment has been in the 80s, they have lost significant money and when it is above 100 the school makes a nice profit. In the past, losses have been covered by generous donations, but donations are far less when enrollment is up, and the need is less.

Activity:

Discuss the risk tolerance of your organization. Bring in its culture and any other factors that would influence how much tolerance the organization might have.

C. Case study 3, Risk Tolerance

Ace electrical had never had a risk management program when the idea was broached by Susan Smith, CFO. When she discussed the concept with Bud, his first reaction was negative for two primary reasons. First, he said that he understood the risks of his business since he had been in the industry all of his life and had built a successful organization. In addition, he said that he was good friends with a bank vice-president who was always complaining about the bureaucracy that had come upon the bank with the advent of an involved risk-management program. His exact quote was, “If that’s what you are suggesting, I want none of it.”

The organization has a power culture with Bud having the say in most things; however, he understands the idea of a team culture and is working hard to move the company in that direction. The subject has been discussed in several senior management meetings, and Susan used that idea as her primary argument for developing an ERM program. She explained that in a well-organized program two things would happen. First, risk management will allow Bud to transfer some of the risk decision making out to the teams. Since he wants to move into more of a team culture, he was very positive about that idea. In addition, Susan convinced Bud that they would be using a risk management system for smaller organizations and it would avoid the bureaucracy often found in financial services companies.

At the outset of the program Susan brought the senior team together to discuss the risk tolerance of the organization. They all agreed that as an entrepreneurial organization it was relatively high. She passed a paper around to the group and asked them to rate on a 1-5 scale, in their own opinion, what the risk tolerance should be. She was surprised to discover that the lowest was 2.5 and the highest was 4 with an average of 3.7. They discussed the results considerably and determined that theirs was a relatively high-risk organization, but they had to make sure that they were being properly compensated for the risk in the form of organizational return.

When Bud discussed risk management with his banker friend, who was also the primary lender to Ace, he learned that the bank annually does considerable analysis to measure the company's risk in the opinion of the bank. They look at several ratios, and the banker agreed to share that information with Susan. The conclusion was that, while the management team would manage risk; in reality, it would also be monitored by the bank if they wanted to continue to enjoy a line of credit and other financing.

Risk Identification

Risk Identification

Learning objectives

Upon completing this chapter, the reader will be able to:

- Know how to identify risks;
- Understand the risks of risk identification;
- Understand who is in the best position to identify risks; and
- See various methods of risk identification.

I. Risk identification mistakes

Now that we have a plan in place and recognize that our organization should practice an organized system of risk management, we need to look to see if we have any risks, where are they located, how severe they are, and how they can be mitigated.

An easy way to introduce the identification process is to discuss some of the greatest mistakes that have been made in the area.

A. Failure to recognize risk early when it is less expensive to mitigate

Little risks often become big risks if not recognized and addressed. For example, let's say that we are a hotel. We need to hire customer service people who have a positive attitude and great skills in dealing with people, some of which may arrive at our hotel tired and have had bad experiences with previous travel that day. In short, they are in a bad mood and may be difficult. Obviously, we face some severe reputation risks given this modern day of online reviews.

Over in our human relations department, we set the standards for hiring and those standards also involve risk. If we make mistakes in interviewing, we face risks involving discrimination claims. Consequently, we might try and minimize those risks by choosing a route of hiring based on totally objective standards such as testing and education; however, that practice could easily allow us to hire people who test well but have poor attitudes and don't handle people well. So, attempting to minimize our employment risk could cause us to have greater reputation risk.

B. Failure to take an iterative approach

The key to the iterative approach to risk management is to avoid taking an irreversible decision now which could prevent a better decision in the future. Another way to explain it would be to have a strategy to keep your options open for as long as possible.

For example, most parents will face an interesting issue of risk management that can be a teaching moment with a child. The issue is, "What should I study in college?" That is a key decision requiring a lot of thought, but it is toward the end of the decision-making plan. The first decision is, "Should I go to college?" That decision is paramount, but actually is preceded with questions about what courses should I take in high school? If I want to keep my options open about the college career, I need to make the decision to take the necessary prerequisite courses for college admission.

Once I've decided to take college preparatory courses, and decided I should go to college, then I'm ready to determine to which college I should go. Obviously, there are a lot of sub-decisions and risks to determine around grade level, financing, and other expenses. Those all should be determined when looking at the risks and rewards. With today's high cost of higher education, more parents and students should probably do some rate of return analysis on which college to attend, costs, and which jobs might become available.

Finally, the decision is about what to study. Again, the decision is often made based on interests, but a risk management approach would bring into play the marketability of the degree. All of this discussion is an example of an iterative approach to risk management and decision-making.

C. Risks are not identified with the appropriate stakeholders

Risk identification is obviously a key aspect to an ERM program. If you don't identify the risk, you obviously can't evaluate and mitigate the risk. But who knows the risk best? Is it senior management or is it the people who are closest to the risk? Generally, it is the latter. Remember the earlier stated concept, "Monitor centrally, but manage de-centrally."

Let's look at our two case studies. If we believed that there would probably be certain risks of children hurting themselves on the playground, then who would be best to identify those risks. Obviously, the teachers who take the kids onto the playground. Probably senior management or the board would recognize that there are risks, but certainly do not know the details.

In the case of the Ace Electrical Products, there are probably a few types of risk associated with selling to the customers. Who would best know those risks? Would it be the senior management or the sales staff? Obviously, the sales staff would be in a better position to identify the risks.

1. Appropriate stakeholders and culture

The organizational culture will have a tendency to influence the possibility of this mistake being made. The Power culture will have a tendency to try and identify risks at the highest levels, and the role culture will often be similar. It will be the team culture that will be more comfortable to empower the people at the lower levels to take on the risk identification process.

D. Not using a variety of risk-identification techniques

There are many different techniques designed to identify risks, and many of them will be discussed in this chapter. The key, however, is to know several of them and use them when the situation will best be served by the particular technique. For example, one team might be best using a SWAT analysis whereas another team will be more comfortable with a brain-storming technique. Since most of the methods yield similar results, I personally suggest allowing the team to pick their own method. Risk identification usually works best when the team is relaxed, and everyone is comfortable in being open and honest. If a particular method has been required, they will sometimes be restricted. That will often occur in the role culture.

E. Risks are not captured in one place

A very frequent problem in a risk management program is that it is managed de-centrally, and then monitored de-centrally. That will not work. While the best way to do things is to count on the teams closest to the potential problems to be the first line of risk identification, it is a big mistake to monitor the risks at that level. Yes, the teams will want to keep their own eyes on their own risks, but the entire risk profile of the organization must be centrally located at one location. In this, and only in this way, can the organization have a good view of the total risk profile of the organization. This is probably the greatest difference between old-style risk management and ERM.

F. Failure to make risks visible and easily accessible

Like anything else in an organization, risk management can be political. Consequently, in some organizations people do not want others to see their “dirty laundry,” which might affect the risks that exist at the team level. This would most likely occur in role cultures. The task of the centralized risk manager, who will probably be the finance professional in small organizations, is to make sure that the total risk profile is available for inspection and evaluation by all people with a need to know.

G. Risks are not captured in a consistent format

As we identify risks, we write them up as “risk statements.” These are statements that tell:

1. What could happen?
2. Why could it happen?
3. Why do we care?

Another way of stating this is:

1. Cause.
2. Risk.
3. Impact.

It probably doesn’t matter a whole lot which format, (or another one for that matter) that you use, as long as you are consistent throughout the organization. If one team uses a particular format, and is not followed by another team, then reporting to the centralized spot can be very confusing.

II. Criteria for risk identification

A. Timing

As we are identifying risks, we have to ask ourselves an important question that has to do with time. Is this a risk now, or could it become a risk in what time frame? For example, every organization has the risk that the CEO will leave the company. The consequences of such an event might be very different depending on the timing and circumstances; however, it does involve a risk. Timing complicates the evaluation of the risk. What is the risk that she leaves the company in 1 month? 6 months? 1 year? 5 years? 10 years? Obviously, the risk increases as the time period increases, but what time period should you use when identifying and evaluating the risks?

The answer to the question is obviously up to the company; however, it should be discussed, and the decision widely disseminated and be used consistently as risks are identified.

B. Ultimate cause

When identifying risks, we should make every attempt to identify the root cause or root risk rather than a secondary risk. There are many examples of this concept, but we will pull one from our electrical tool company. Certainly, the sales team would identify that there is a risk that a product would not be acceptable to a customer and wouldn’t work as it is intended. That is a risk of the salespeople, but the root risk is more about the risk that the quality is not sufficient. That risk would probably be identified by the team dealing with the supply chain. Both risks should be addressed, but probably the supply chain risk is more immediate and can be mitigated through quality control whereas the customer risk has more to do with mitigation than having to do with sales returns and customer satisfaction.

III. Identifying risk in management layers

A. Senior management

For example, in this case we will say that the senior management team of the company consists of the CEO, CFO, COO, CMO, and CIO. Obviously, there could easily be others in the C suite of the company, but for simplicity, we will use that list.

As a team that group should be responsible for identifying the overall risks of the company including such things as strategy, future planning, and overall direction. When the team meets to identify those risks, it should refrain from getting into the details, but concentrate on the overall policies.

Interestingly, I have found that often some of the areas that require the attention of this group are the ones that are not even discussed. For example, there is a particular risk that is often forgotten which is called innovation risk. This represents the risk that some other company is going to completely change the way business is done, and consequently we may run the risk of going out of business. Despite the fact that we are changing very quickly today, we usually see these kinds of changes well in advance, but often are unwilling to recognize the risk.

For example, for several years traditional retail has been under attack from online retail and Amazon. Have retailers seen it coming? Of course, but often they have been unwilling to recognize the risk and do anything about it. In the same way, it is well known that the Kodak company recognized the innovation of digital photography well in advance of its popularity; however, it has been reported that senior management was unwilling to deal with the risk. Decisions like this will cause even the largest companies to fail.

B. Level two

The second level of the organization will consist of teams responsible for the particular major areas of the company. The CFO will head a team consisting of the heads of each of the specific areas of accounting and finance. The CMO will lead the marketing team probably consisting of the sales manager, advertising manager, and other similar areas. The COO will lead the team dealing with operations, and the CIO will lead the information team.

Risk identification will fall on those teams for the overall risks related to their areas. For example, the finance and accounting team will have the overall responsibility for identifying financial risks, and the COO will head up the team identifying operating risks. Obviously, the CIO will be most interested in cyber risks.

C. Level three and more

Each of those larger teams will probably have sub teams that will identify the risks under their control. For example, the finance team may have a person in charge of collection and head up a collections team. There are a lot of risks having to do with collection, and those people on that team should be the ones responsible for identifying those risks.

Obviously, the identification doesn't stop here. Depending on the size of the organization, teams all the way out should be convened to discuss and identify the risks in their specific area. For example, who is the best one to identify the risks in driving a truck for the company – some senior manager or the drivers themselves? The answer should be obvious.

IV. Identification methods

Regardless of at what level the identification takes place, there are several possible methods for the team to use in its search for determining all of the important risks. Before getting into the methods, let's consider two related problems that need to be overcome.

A. Potential problems

1. Politics

Regardless of how we configure a risk management program, organizational politics come into play. Our desire is to determine all of the significant risks so we can attempt to mitigate them; however, sometimes people are protective of their "turf," and won't be completely open. People who are particularly controlling can easily become defensive and not want to admit that there are risks in their areas – especially ones that they may not have addressed. This is most likely to happen in the role culture.

2. Need for team

Because of problem 1, we have a great need for team. Risk identification must always be done in a team format where there are several people knowledgeable of the area who will openly and honestly give their opinions of the risks. For this reason, all of the methods listed involve teams and are designed to get people to be open and honest with their opinions about potential risk. In fact, the total success of the risk management program depends on well-working teams.

B. Methods

All of these methods are best accomplished when the team is in a controlled atmosphere, away from distractions, and is able to concentrate on the task at hand. This should often be in an offsite location.

1. Brainstorming

Here the group is instructed to make a large list of all possible risks that might be faced in the particular area of interest. As said above, the senior management would be looking at more strategy issues, and the people in the teams furthest out from management would look at their own particular disciplines. It is important to note that in brainstorming, the ideas are NEVER to be discussed as they are listed. The reason – we want ALL ideas, no matter how outlandish, to be listed. We will have ample time in the next step to discuss the ideas to make sure they make the final cut. If this rule is not followed, the more timid and less assertive members of the team may not submit ideas because they think they will be harshly ridiculed.

A way of stimulating more possible risks to be listed would be for the team leader to ask probing questions such as, "What would happen if: we lost power, the premises were not available, suppliers went out of business, or there was a natural disaster?"

In the brainstorming phase leaders will often be sure to include some obviously outlandish and "stupid" ideas on the list. This is done to show that there is no such thing as a stupid idea in the brainstorming phase. By being vulnerable, the leader will encourage the group to be more open and not refrain from adding something to the list that they might think was “stupid.”

2. NGT (nominal group technique)

Once all of the ideas are on the board, they have to be weeded out to eliminate the ones that will not be discussed. The most obvious way is to go through a cross-out system where each idea is discussed, and some are eliminated by consensus. Another way is to have each member of the team rank each idea on some type of scale such as 1-5 where 1=best and 5=worst. Then rank all the ideas by total score and discuss which ones should be eliminated.

3. Checklists

In risk management literature there are a lot of checklists available that will allow the team to be sure to include risks in particular areas. These can be very important to avoid missing risks in obvious areas but that could possibly be overlooked.

4. Assumption analysis

Assumptions are factors that are considered to be true, real, or certain without proof or demonstration. We just “assume” that they are correct. Assumptions are key sources of risk and need to be discussed. This can be done with a simple question for the group such as, “What assumptions do we have concerning this project?” Then, we document the assumptions and the associated risks involved.

C. SWOT analysis

This is probably the most common tool used for risk identification. It should always be used at the higher levels of the organization but may work well at any level. The greatest advantage is that it tends to separate risks between internal and external with the internal ones being ones that can generally be controlled and external being risks that cannot be controlled.

1. Internal

This part of the SWOT analysis are our strengths and weaknesses. They belong to us and generally can be controlled by us. If we have a strength, generally we want to recognize that there is risk that the strength be maintained. If we discover a weakness, then we want to obviously ask about the risks that the weakness could cause and ways to overcome the weakness. These might include such things as human risks such as health, theft and fraud, morale, and turnover. These risks would also include information and technology risks.

2. External

These are the items under opportunities and threats. They are external to the organization and generally we can’t control them. However, we can do things that will exploit and expand the opportunities and avoid or mitigate the threats. For example, if we were thinking of building a plant in the central part of the country, we would want to consider environmental risks. There are hurricanes on the Gulf Coast and tornadoes on the Central Plains. Some, but not all, of those risks can be insured, but insurance costs may change, and the risks must be considered.

Activity:

If you were part of the senior leadership team of the private school, what are some of the risks that you might consider? Use the SWOT analysis method.

V. Conclusion

There are many more methods and tools used for teams to uncover risks, and they are available through further research if desired. The important thing to recognize is that if a risk is not identified, it will not be mitigated. The first, and most important part of the process is identification. Use whatever methods desired but use some method that will push the teams along to identify all of the risks.

Risk Evaluation and Assessment

Risk Evaluation and Assessment

Learning objectives

Upon completing this chapter, the reader will be able to:

- Understand how to evaluate risks;
- Know various methods of risk evaluation;
- See how the risk matrix works; and
- Understand risk classification methods.

I. Key point

In the prior chapter, we discussed ways to identify the risks in the organization; however, we made no attempt to evaluate them. We just identified the risks without saying if they were large or small risks, the impact on the organization, or even how often they might occur. In this chapter, we will attempt to fill in those blanks.

Risk assessment involves the recognition of risks and rating them to attempt to determine which are most significant to the organization.

Many organizations spend a huge amount of time and effort in identifying and evaluating risks, but then fail to arrive at a good strategy to somehow mitigate those risks. The practice is only useful if it sets the stage for informed decisions to respond to those risks. Identification and assessment are useless unless those steps are followed up with sound mitigation responses.

Why does the mistake of not following up with mitigation often happen? For many reasons, but probably often because many people see many of the risks facing the organization as inevitable and impossible to resolve. Consequently, they take on the “ostrich” effect and pass the risks off as being unfixable. An example occurred several years ago to a major photographic film manufacturer. Many people in the organization saw the advent of digital photography and recognized the risk to the entire strategy of the company. They talked about it and passed the discussion up to senior management. But senior management was so “married” to film that it was unwilling to take the early steps to prepare for the change. That decision almost cost the company everything and was probably due to internal corporate politics.

II. Difficulty of assessment

It is not easy to accurately assess the severity of risk primarily because it is a subjective exercise. One person asks another, how risky is that? The answer may very well be something like, “not too risky.” Analytical people do not like that response and will often request that the person quantify the answer in some way. That can be done, but let’s remember that it is still subjective, and the answer is apt to differ from one individual to another. We will attempt to overcome this difficulty by involving many people in the process and use a rating system enabling us to make a subjective concept more objective.

Another big problem is that one risk is not like another. The risk of a major change in the business model creating a risk in the company’s strategy is totally different from the risk of a child falling on the playground of the school. But somehow, we need to arrive at a system to bring “apples and oranges” together in the evaluation process.

III. Approaches to risk assessment

The basic approach to the process of risk assessment is to gather together (in-person or virtually), a group of people who should be most familiar with the potential risk. Then, we will have those people attempt to rate the severity and likelihood of the risk on some type of numerical scale and average the numbers for a final result.

A. Where should the evaluation take place?

The key throughout this program is the concept that we should monitor risks centrally but manage them de-centrally. Consequently, the evaluation should take place at and with a group of peers who would be in the best position to truly understand the severity of the risk. In the prior chapter we mentioned that obviously the teachers on the playground of the school would probably be the best to identify the risks that could happen to the students and staff. If they are the ones to identify the risks, shouldn't they be the best to evaluate the risks? The answer is obviously yes. On the other hand, the senior management team would probably be the best to evaluate the risks involving the primary business model and strategy of the organization.

But, how do we make sure that the practice is accomplished? The answer is that the process must be managed centrally with one person in charge of making sure that risk management happens, and those teachers do, in fact, identify and analyze the risks.

B. Top-down or bottom-up

1. Top-down

This approach is more likely to result in an enterprise-wide approach since the risks at the top will be identified first and recognized to have impact down through the organization. With senior management and the board first engaging in the project, the rest of the staff will recognize its importance and be more apt to "buy in" to the project. Also, since the project starts at the top, there will be a greater tendency for everyone to follow a uniform methodology.

The approach can also have its disadvantages. Senior management and board members have a tendency to concentrate on risks external to the organization; whereas, middle and lower management will be more likely to recognize internal risks. Therefore, risks emerging from the operations of the organization may not be fully identified and evaluated.

2. Bottom-up

With a bottom-up approach the organization is more apt to have complete buy-in at all levels. Operational staff will have great awareness of local risks and their causes and be in a much better position to mitigate the risks. While methodology can be varied according to the local norms, as long as well managed, this can be useful in a multinational organization.

A big disadvantage to this approach is that the external risks may be less emphasized. Most of the risk-management effort may be at the staff level and those individuals may not see the outside picture. In addition, if politics are involved, and they always are, there is a danger that some of the risks will not be brought to the attention of senior management.

3. Conclusion on this issue

For most organizations, a combination of top-down and bottom-up should occur. The external strategy risks that are identified by senior management must be identified and evaluated as the details cascade throughout the organization. Senior management needs to be totally involved and set the example for the remainder of the staff. But, at the same time, senior management should allow the creativity of the other teams to identify and evaluate the risks that they see in their respective areas.

IV. Risk assessment techniques

A. Questionnaires and checklists

This technique is widely followed by many organizations and has the advantage of being able to be used virtually, give respondents plenty of time to evaluate, and create involvement in a large number of people. The disadvantages, however, are significant. In many organizations, people do not respond to questionnaires in a timely manner, and a lot of follow-up is often required.

B. Workshops and brainstorming

This is one of the most popular methods, but very expensive in cases of decentralized organizations. The advantage is the synergy of many individuals being creative where one person’s ideas build on another’s. When properly run, workshops tend to break down politics and people are honest with their opinions. However, in many organizations, gathering a team together to talk about risk management will require people being away from their daily duties thus affecting productivity. Can you imagine the effect on a large trucking company if all of the drivers stopped driving for a couple of days to discuss risks? Another key problem is cost. Bringing the sales staff together from places around the world to discuss customer and market risks will cost a lot of money.

C. Inspections and audits

Physical inspections and audits can be very effective in uncovering certain types of risks, however, may miss others. Physical evidence can quickly form the basis of opinion and will often uncover risks of a more physical nature such as the risks of the children on the playground of the school. However, audit inspection can tend to concentrate on historical evidence and not look into the future. This technique is probably more useful in the operational end of the enterprise and not a lot of use in evaluating the business model and strategy.

D. Flow charts

This technique is almost required at the operational level of the organization. By analyzing a flow chart of a process, such as the supply chain, the staff is able to see the risks of critical components. Another advantage is that the output can often be used as a risk-assessment tool for other parts of the organization. The disadvantages are that the technique is relatively useless for strategic risks and may be very detailed and expensive.

V. Risk matrix

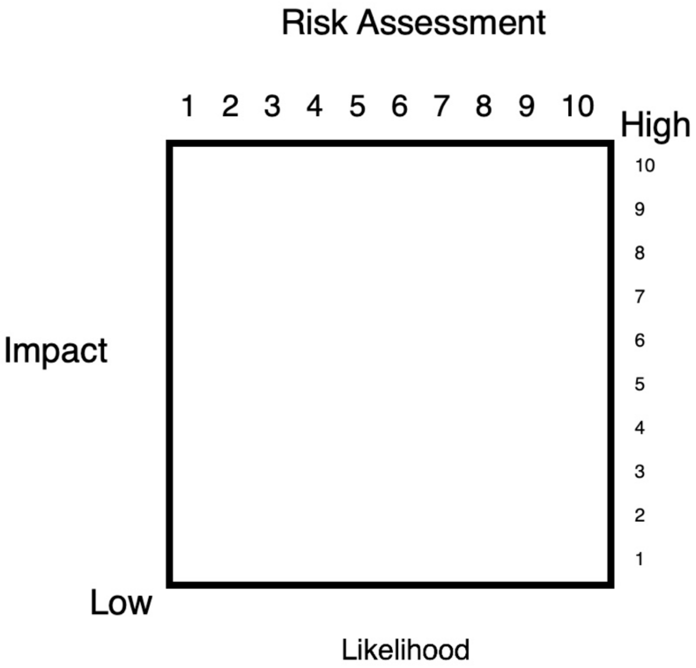


Figure 4-1

The above matrix shows a commonly used tool for evaluating risk in an organization. Any defined risk can be evaluated over two important criteria – impact on the organization and likelihood of occurrence. The organization will have to define those criteria but following is a commonly used one.

A. Frequency

1. Unlikely

In this case, we could expect that the occurrence is very unlikely and probably has occurred only 2 or 3 times over the past 10 years.

2. Possible

This item has occurred in this organization more than 3 times over the past 10 years and is certainly possible in the future.

3. Likely

This item has occurred more than 7 times over the last 10 years or circumstances have arisen that will cause it to happen in the next few years.

4. Almost certain

This item has occurred 9 or 10 times in the past 10 years or circumstances have arisen that will almost certainly cause it to happen in the near future.

B. Impact

1. Small

This item would have almost no impact on the customer or organization. There would be a minor reduction of reputation in the short run, would incur no violation of the law, and have a small impact on the economics of the organization.

2. Moderate

A moderate exposure would represent something that caused a relatively minor temporary impact on a customer or the organization, a small reduction in reputation for a short time, possible violation of a minor law resulting in a warning, and a small economic loss to the organization.

3. Severe

This event would have a serious impact on a client, customer, or the organization. It might influence trust such that it would have a major impact on the reputation of the organization or major laws could have been broken. This event would represent a large economic loss.

4. Catastrophic

This occurrence might cause death to an individual or the organization. The reputation of the organization would be devasting and it could be a serious violation of law. The event would cause a severe economic loss to the organization calling into question its viability.

Obviously, the exact wording of these criteria would differ with each organization; however, it's important that everyone in the risk management process agree upon the definitions and use them consistently.

VI. Using the matrix

The object of the matrix is to discuss each identified risk along the two criteria of impact and likelihood. The best way to accomplish the task is have the members of the team have an open and full discussion of the two items, and then in ballot fashion, ask the members to score the two criteria in the form of a 1 to 10. In most cases, you will find the ratings to be very similar and can be averaged to give a final rating for that particular risk.

Activity:

In a small group identify a risk that might be somewhat similar in all of the organizations represented. Then, for that risk, discuss its impact on the organization as well as its likelihood of occurrence. Then, in ballot fashion, ask each person to rate both the impact and likelihood on a scale of 1-10. Discuss the ratings, the system, and if this system would work in your organization.

VII. Risk classification

A. Time-oriented systems

Many organizations classify their risks into short, medium, and long-term. In this way, they often will identify risk into those being related to operations, tactics, and strategy, respectively.

1. Short-term

A short-term risk has the ability to impact the objectives, dependencies, and core processes with immediate impact. These risks can cause disruption immediately. An example might be the closing down of a major supplier or a fire destroying a warehouse. This would be seen as an operating risk and need to be addressed by those most familiar with operations.

2. Medium-term

This type of risk has the ability to impact the organization following a short delay after its occurrence. Typically, the manifestation of the occurrence would not be immediately obvious but would become apparent within months or at least within a year. The addressing of this type of risk would be more of a tactical nature. An example of a medium-term risk might be the introduction of a new product by a competitor at a significantly lower price.

3. Long-term

Long-term risks have the ability to affect the organization well after the occurrence of the event. Long-term risks usually impact the ability of the organization to maintain the core processes that are concerned with the development and delivery of the core strategy of the organization. An example of this risk might be when Kodak faced digital photography.

B. FIRM system

Over the years of risk management there have been many classification systems including the COSO ERM cube, the IRM standard, and the FIRM risk scorecard. Should your organization be operating under one of the systems, it is important to fully understand it; however, since this course is designed for smaller to medium-sized organizations, it is assumed that such a classification system has not yet been developed. For this reason, we will use the FIRM system which is one of the easiest to use in a small business. FIRM is an acronym for financial, infrastructure, reputational, and marketplace.

Before we begin to discuss the four areas, it's important to recognize how financial is defined. A good case can be made that every risk, of any type, is a financial one. This is because an adverse occurrence of almost any type will eventually have an adverse effect on income, which will eventually affect the financial statements and all of the financial ratios. But, for this classification system, financial is defined in a more specific fashion.

1. Financial

These are risks that can impact the way in which money is managed and profitability is achieved. Financial risks are primarily internal, usually quantifiable, and can be observed and determined by gains and losses from key indicators. The primary way of controlling the financial risks is through various controls such as capital expenditure, spending, cash controls, and similar items. Fraud or defalcation is a common type of financial risk.

2. Infrastructure

These are risks that will impact the level of efficiency and dysfunction with the core processes of the organization. For example, if the manufacturing plant were to be destroyed by a tornado, the efficiency of manufacturing would obviously be significantly disrupted. In the same way, however, should an employee in a key position be taken ill for a long time, that also could be considered a risk affecting efficiency. This risk is usually internal and sometimes quantifiable. The key measurement to determine how the organization is doing regarding this kind of risk is various efficiency measures. These risks are normally controlled and mitigated through loss control, insurance, and process controls.

3. Reputational

Reputational risks are risks that will impact the desire of customers to deal or trade with the organization. They are external in nature and are very difficult to quantify. The key performance indicator for this kind of risk will be the nature of the publicity and effectiveness of the marketing profile of the company. Since this kind of risk is difficult to measure and quantify, it is less often addressed by many organizations.

4. Marketplace

These are risks that affect the level of business done by the organization. It is an external risk and quantifiable by income measurement. However, it is important to recognize that marketplace risk often has a large lag after the occurrence of the risk event. For example, the advent of Amazon in retail is certainly an example of such a risk; however, many traditional retail stores did not feel the financial effects of the competitive environment for several years.

C. PESTLE system

PESTLE is an acronym for the following risk factors. Using this system, at each level of the organization, the team would categorize the risks with these factors.

1. Political

This area would include tax policy, employment laws, regulations, trade restrictions, tariffs, and international risk.

2. Economic

These risks would include things like recession, inflation, interest rates, wage rates, working hours, and similar items. It’s interesting to note that several of these items could also be considered under political since politics will often determine such things as working hours and wage rates. Economics and politics go hand in hand.

3. Sociological

This category of risks would include such things as cultural norms, health considerations, demographics, career attitudes, educational attitudes, and similar items.

4. Technological

Changing technology causes a huge amount of risk that would be considered under this heading. Technological changes may affect your products or services, barriers to entry into markets, and even what products and services will be available in coming years.

5. Legal

Changes to legislation that could affect your products or services could be considered either under political risk or legal risk. Similar risks would involve employment, liability, tax, and even the cost of legal representation.

6. Ethical or environmental

Although often different, the two items are often combined since many people consider how our firm affects the environment to be very much of an ethical issue. Many of these risks will also be sociological or economic and even technological.

7. Addendum to PESTLE

It is interesting to note that the PESTLE system does not include financial risks as a category. As financial people, we may very well dismiss this system since we know that financial risks are significant. The reason is that the PESTLE system understands that all risks will end up affecting the financial condition of the company, so specific financial risks are included under the other headings.

Activity:

In a small group, discuss the possible risks of a small, faith-based school using the PESTLE classification method.

Risk Response

Risk Response

Learning objectives

Upon completing this chapter, the reader will be able to:

- Know best how to respond to risks in various situations;
- Understand how to determine what risks to insure;
- Understand responses to positive risks; and
- Have more understanding of the risk matrix.

I. Revisiting the matrix

We have identified risks, analyzed their significance, and now we are in a position to formulate a plan to deal with the risk. While we will do much of our thinking about negative risks, we must not forget the risks of positive occurrences. We need a plan for both. This chapter will be broken into two specific parts with the first dealing with theoretical plans meeting different situations, and the second part being a case study using the fictitious school as an example.

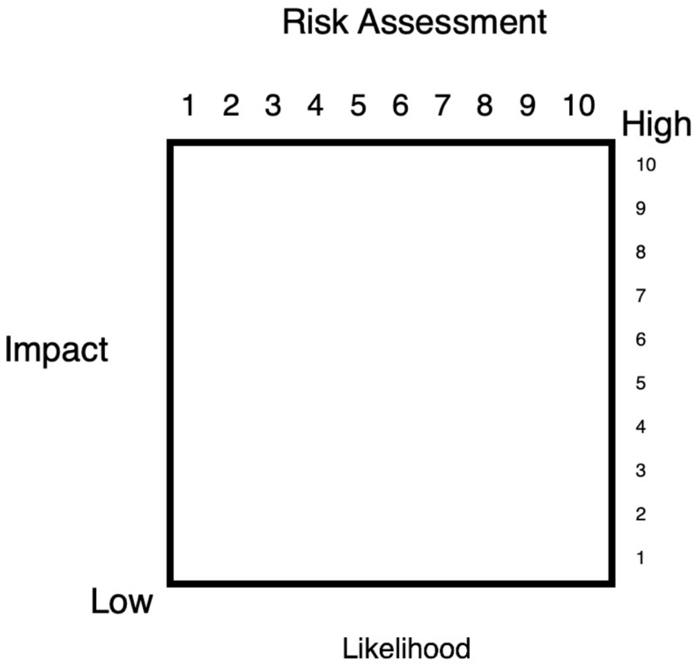


Figure 6-1

You will recall that we determined that we should rate risks from the standpoint of their severity to our organization based on the likelihood of occurrence and the impact of any occurrence on our company. This is shown in Figure 6-1. Now, let's look at the same matrix with an initial concept of the plan that could be developed for each of the possible severity measures. (Figure 6-2)

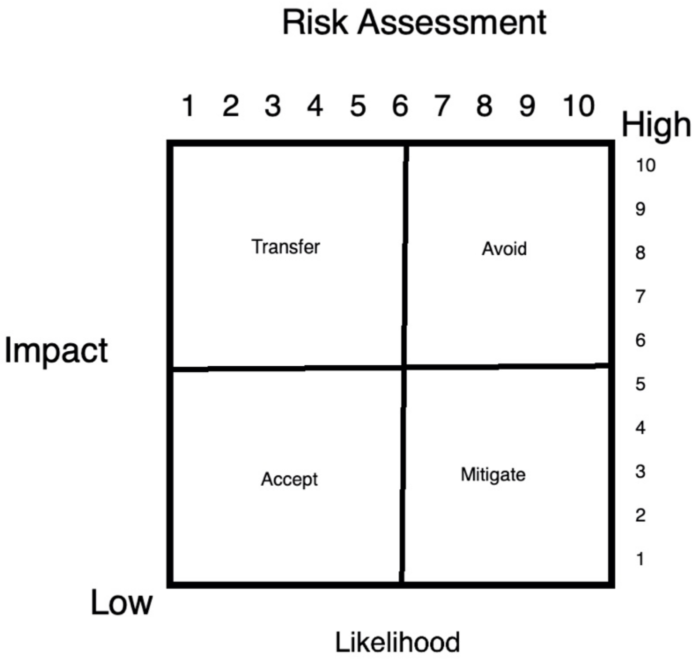


Figure 6-2

Before we begin, let me emphasize that what we are discussing is not an exact science, and therefore does not work in each and every situation; however, the concept works the majority of the time to the point where it should be examined as a system.

A. Low likelihood and low impact

These are the risk items of our organization that represent the risks of doing business and about which we can do very little. While not always, they tend to be external factors. While we might not like things like shoplifting in our convenience store, certain weather events, employees arriving late or taking unscheduled time off, and similar items; they are part of doing business and we must learn to live with them.

1. Monitor

You might easily ask if we should even consider these risks since they would rate low in the numbering system; however, we do need to have a plan for them. Generally, we monitor their occurrence. Shoplifting, or inventory shrinkage is an important ratio that we should be monitoring and tracking. The same goes with employee turnover, absences, and accidents.

Ratios are a key part of our monitoring and management system dealing with these kinds of risks. For example, if we are a lending company, a certain amount of loss is expected; however, loss is a risk. How we manage that risk, is through a loss ratio such as amount past due divided by total loans. If that ratio should inch up, we can quickly manage it through a discussion of our credit policy.

2. Active or passive management

With items that do not happen all that frequently, or have relatively little impact on the organization, we cannot usually afford to actively manage them, especially when we consider costs other than direct financial costs. For example, we may know that a small amount of theft occurs in our office with employees taking home an occasional yellow pad or pencil. Is it theft and is it wrong? Of course, but putting in a system of searching each employee as they leave for the day is not only expensive but would have a huge negative impact on the organization's culture. Consequently, we watch our supplies expense over time, or even compare it to other departments.

3. Have a plan

For this type of risk, it's important to have a plan to keep the loss down to a reasonable level or a plan to reduce the expense. These plans are often around cultural improvement. Many successful companies have Chief Culture Officers who know that culture is possibly the key factor for the organization's success. Consequently, when any control, rule, and procedure is put in place culture is considered as an expense of the decision.

4. Rules vs. principles

It's important to recognize the difference between rules and principles and the effect that difference has on the culture of the organization. In our effort to plan for these issues, we establish rules that we think will reduce the expense and improve the situation. For example, one risk that we might have is that our sales force will cheat on their expense accounts thus causing higher travel and entertainment expenses. Some organizations will take a "rule" approach to attacking this risk and put into effect a lot of regulations and rules about travel. They might restrict which hotel in which to stay, which car to rent, and have very detailed T&E expense reimbursement forms.

Other firms will take a more monitoring or principles approach and monitor the amount of T&E divided by sales. With that approach, the financial executive can drill down when the T&E expense/sales ratio is too high. The latter approach tends to cost less and results in a better culture where the sales force will be less inclined to cheat on their expense reports.

B. High impact, low likelihood

These are risks that have a low likelihood of occurrence, but if they do happen, it can spell disaster to the organization. While not always, many of them are external in nature, and we can do very little to stop the occurrence. But we can mitigate the damage through proper planning and often transfer the risk. With any high-impact risk we need to somehow avoid the risk; however, when chance of occurrence is relatively low, it may be economically feasible to transfer the risk. The most obvious method of doing this is with insurance.

Some examples of these types of risks include but are not limited to: severe weather and storms, liability claims from accidents and other items such as data breaches, employee claims, and severe supply chain problems. We will cover many of the details in future chapters, but in this chapter, we will discuss the broad issues of how to handle the risks through transfer.

One broad thing to consider is that it is almost always expensive to transfer risks, so the key becomes the economic tradeoff between the risk and the cost of transfer. The best example of this is the cost of insurance. If we have a fire, its impact would be devastating, and its likelihood of occurrence would be relatively low. Thus, it is probably economically beneficial to insure for the fire loss including any loss of business costs of being without the facility.

1. Insurance

Insurance is a separate, and highly specialized discipline and won't be covered in detail in this program; however, we do need to discuss a couple of key aspects. The first is that the insurance company has to make money and wishes to make a profit. Consequently, in most situations, when we can afford the loss, it is more economical to self-insure for the loss. But that is only in the case of the very large organization that can withstand the loss. For the smaller company, insurance with an insurance company is required. So, where is the cut off?

One concept that I learned a long time ago is to:

Never ensure a loss that you can afford to take.

Are there exceptions to this rule? Of course; however, in most cases it is a good principle. The exceptions will be where having the insurance includes other benefits that reduce other costs. For example, in many cases insurance will assist the company in loss mitigation since they have assumed much of the loss. Insurance company experts will visit, recommend fire prevention techniques, spot accident risks, and similar things. It is because they are experts and the company usually is not.

Another advantage of insurance may be legal representation. In the case of an individual, possibly the greatest benefit of having automobile liability insurance is that if you are sued, the company's attorney will fight the battle.

It's funny how many people will violate this principle in small things like extended warranty programs. Essentially, they are a form of insurance. If the company is buying a computer for $5,000, should you purchase the extended warranty program? No, as long as you could afford the risk of the $5,000 loss. We find that a lot of companies will make this mistake because department heads don't want the personal risk of a loss, although for the company, the risk is not significant.

2. Contracting

In many cases a company will not want to deal with certain employee-related risks. Hiring entails potential discrimination lawsuits, employees expose the company to injury lawsuits and workers comp claims, and specific industries can require specialized knowledge that the company may not have. Many of these kinds of risks have great impact, but the occurrence is relatively low. Consequently, the company may wish to transfer the risk to a contractor who assumes the risk and provides the service to the company. Naturally, the contractor will want to make a profit, but they may have greater knowledge in assuming that risk.

An example of this may be that you are a highly specialized technology company with a relatively small staff of very highly paid employees. But you have to keep your office clean. Cleaning employees are a totally different group than you have had experience in managing. Consequently, you transfer the risks on dealing with those employees through contracting with a company to clean the office. Could you clean it for less? Sure, but do you really want to have the risk?

Another example is IT risk. Do you want to have a server in your company with the risks it entails, or do you want to rely on the cloud to house your data? While the cloud is often more expensive, it is probable that the cloud companies are more experienced to prevent data breaches.

3. Partnerships and joint ventures

Similar to contracting, often other organizations are more experienced with dealing with risks of a certain nature. In international commerce, for example, the company may wish to form a partnership or joint venture with another company in a foreign country that has experience in that culture. You will recall that Ace Electrical Products imports tools from China and distributes them to electrical supply distributors throughout the US. Should they have a break in their supply chain, the effect would be devastating. But this is not the kind of risk that they could insure. Consequently, entering into a partnership or joint venture with a Chinese company might be a way to transfer that risk. Of course, entering into such a partnership obviously brings about other important risks.

4. When you can't transfer

The recent pandemic is probably a good example of a risk that had a very low likelihood of occurrence and a high impact on the organization. Pandemics are usually exempted from insurance policies, so transfer mitigation is relatively impossible. The answer for this mitigation is to reduce the impact on the organization as much as possible by making it more nimble for change and doing other things that allow you to quickly shift to work-at-home arrangements and similar strategies.

C. High likelihood, low impact

These are the kinds of risks that we face every day, and it is way too expensive to transfer the risks. They are of moderate importance to the organization and therefore, we work hard to find ways to manage them and attempt to mitigate their effect. In fact, this is where most of the management of an organization rests. A loan company will receive payments late. That is a risk worth managing. It will do so by shifting its credit standards. A mail-order retail company will have complaints from customers. It will manage those complaints through training of the customer service representatives. An airline will have delayed flights. It will manage that problem through a complex system in operations, but a smart airline will also manage the customer reactions to those delays.

A list of some of the ways we move to manage these occurrences follows:

1. Staff training;
2. Documenting procedures;
3. Controls;
4. Equipment maintenance; and
5. Emergency preparedness.

It is important to note that the organization needs to keep these types of management procedures up to date. Otherwise, we will have plans in the organization that have no real link to real risk. For example, many companies have rules that senior executives cannot travel together on the same airline; however, there is no procedure preventing them from getting into an automobile and going to lunch together. According to probabilities, that makes no sense. More recently there is an example about public schools. States require them to have frequent fire drills, but when is the last time you have heard of a fire in a school? But mass shooter drills are required far less.

D. High likelihood, high impact

These are the items that you must avoid in the organization. Should you do them, the likelihood of disaster is far too great, and the disaster has too great an impact on the organization. You must avoid these risks!

As an example, let's take our case study with Ace Electrical Products. Let's assume that the company has made huge growth and wishes to build a distribution center. To improve its distribution, it would like to locate the center somewhere in the center of the country, but it also recognizes that weather makes a huge difference in such things as delays and even the safety of the buildings and therefore insurance rates. It determines that a tornado is too high an impact risk to endure, so it makes the decision to locate the center out of the traditional tornado high-risk area.

Some of the ways that we will avoid these high impact risks will be:

1. Change business processes;
2. Change equipment;
3. Use different materials;
4. Use a more proven practice;
5. Improve communication; and/or
6. Train to avoid.

An example of the last item has to do with cyber threats. Regardless of our desire to admit it, there are organizations that are trying to break into our computer systems on a daily basis. Some of the breaches are almost impossible to totally prevent, but many of them occur due to stupidity on the part of employees. Proper training of our staff with a lot of examples can train them not to fall for emails and other offers that in reality are phishing exercises from people trying to harm us.

II. Responses for positive risks

While admittedly, we probably don't concentrate enough on the positive risks of the business, it is important to recognize our possible strategies.

A. Low likelihood/low impact

While we would love these things to occur, in most cases they probably won't. We can have either an active or a passive approach to exploiting their occurrence. A passive approach would be to watch for them, and make sure we are prepared to strike should they happen. An active approach would be to have team members out looking for the opportunities. The most successful organizations in R&D will do the latter.

B. High likelihood/low impact

These items come along very often, and when they do, we need to be in a position to enhance them. They don't make a lot of difference, but we should grab them as they occur.

C. Low likelihood/high impact

Because these risks can have such a positive impact on the organization, we need to consider partnering or collaborating with others with more experience or closer to the market to make sure the item happens. In addition, we might consider moving our staff around so that we have our best people or greatest resources devoted to the areas of greatest impact.

D. High likelihood/high impact

This is the bread and butter of the organization. We need to make sure that we have both resources and people in place to capitalize on this side of our business to ensure success.

III. Activity – Case study

In this section we will look at our faith-based private school and analyze the risk using the PESTLE system. For each type of risk, evaluate the possible likelihood and impact, and then discuss strategy that might be followed. Several of the risks follow.

A. Political

Political risks for the faith-based private school might include the following:

1. Changing the state tax system;
2. Changing the deductibility of contributions;
3. Changing home-school requirements; and
4. Changing accreditation requirements.

B. Economic

Economic risks for the faith-based private school might include:

1. Increasing cost of educational materials;
2. Recession; and
3. Wage rates for teachers in public education.

C. Sociological

Sociological risks for the faith-based private school might include:

1. Acceptance by society of faith-based education;
2. Changes in thinking about “inclusive;” and
3. Dress code.

D. Technological

Technological risks for the faith-based private school might include:

1. Cost of keeping up;
2. Availability of home-school curriculum; and
3. Data breach.

E. Ethical or environmental

Ethical or environmental risks for the faith-based private school might include:

1. Discovering environmental health issues in the building.
2. Risks from other people:
   - Teachers.
   - Other students.
   - Other examples:
     - Perfume.
     - Peanuts.
     - Pesticides.
3. Conflict.
4. Assessment:
   - Testing.

Strategy Risk

Strategy Risk

Learning objectives

Upon completing this chapter, the reader will be able to:

- Understand the importance of strategy risk;
- Know why strategy risk is often not considered;
- Know what "destructive innovation" is all about; and
- Understand and react to reputation risk.

I. In general

In some people's categorization of risk management, there are the four categories:

- Strategic risk;
- Operating risk;
- Financial risk; and
- Compliance risk.

While we are not using that categorization system in this program, it is well accepted. It is important to note that the first item mentioned, and by far the most important, is strategic risk.

It is interesting to note that only a few years ago, strategic risk was not generally discussed and not considered terribly important with most of the attention going to operating, financial, and compliance risk. Over the past few years, that trend has shifted where strategic risk is often considered the most important.

A recent survey completed by Deloitte reported that 81% of organizations now actively manage strategic risk rather than limiting their focus to traditional risk areas. The cause of this shift should be obvious – the nature of the operating, financial, and compliance risks can have a major effect on the organization; however, strategy risks can put the organization out of business in a very short time. When we look at the history of large companies that were once on the top of their industries, we often find that some are no longer in business or even that the industry has almost ceased to exist. This chapter will take a close look at strategic risks with a twofold purpose:

- Recognize the great risks of following the wrong strategy; and
- Develop a plan to keep up with changes causing a need for strategy changes

II. Responsibility for strategic risk management

While operating, financial, and compliance risk management is often managed by the operating departments, even though it is monitored at the senior level, strategic risk management must be the responsibility of the Board of Directors and senior management. The size and nature of the organization will usually dictate the level where it is managed.

In many people's view, strategic risk represents by far the greatest risk that the organization faces.

Consequently, it must be addressed at the most senior level of the organization.

For the purposes of this program, we will consider strategic risk in three specific areas:

1. Business model risk;
2. Reputation risk; and
3. Manpower risk.

III. Business model risk

Simply stated, this is the risk that the business model that has been adopted by the organization will fail to achieve the desired results. The primary reason why this occurs is change.

A. Activity

Ask yourself a simple question.

Is our organization changing as fast as the world around it?

If the answer is yes, that's wonderful. If the answer is no, then you have to ask yourself one additional question – what will happen to it? Unfortunately, you will not like the answer because it is that it will cease to exist. Possibly it will go out of business, or possibly it will be bought by another organization that is changing with the world. But, in one way or another, it will no longer be a viable enterprise.

Are there exceptions to this statement? Sure – probably some monopolistic organizations may not face the competition of organizations that do change, but they will be relatively few and far between. All you have to do is look at a couple of examples such as what happened to Kodak with digital photography or most bookstores due to Amazon and you quickly see how changes can quickly cause a business model to be obsolete.

This may be the most important question you will ask in this entire program of risk management. When I have asked the question in live seminars, I generally get about 10% to 20% of the group saying that their company was changing as fast as the world. I plead with you to take this question to senior management and discuss it in detail. That discussion could save your business.

B. Denial at the senior level

For years, Kodak had the lock on photography to the point where their name was almost generic as people sometimes referred to a camera as a Kodak. What happened? Obviously, someone developed the concept of digital photography that was less expensive, far more flexible, and served the market better. It took some time for professional photographers to adapt to the new technology, but now a person would have a difficult time finding a photographer still using film on a regular basis.

How did Kodak miss this development? The answer is that it didn't. Many people in the organization saw the development of digital photography, especially at the lower ranks of the organization. But, according to a former Kodak employee with whom I talked a few years ago, senior management was unwilling to admit that digital photography was more than a "flash in the pan."

C. Concept of destructive innovation

The term, “destructive innovation,” was introduced by Clayton M. Christensen in 1995 and has been called most influential business idea of the early 21st century. Essentially, it represents an innovation that creates a new market and value network that eventually disrupts an existing market and value network. Not all innovation is considered disruptive. For example, the early automobile might not have been considered disruptive because it didn’t replace the carriage due to its very high cost. But the mass-produced automobile would be considered disruptive since it directly competed with the carriage and put it out of business.

Christensen, in several of his books, has carefully defined the term and some people have argued if an innovation is disruptive or not. For the purpose of this work, we will not get into a debate about terminology, but will primarily discuss the need for change due to innovation in general.

D. Not good or bad, it just is

When we discuss innovation in the abstract, most people are in favor and it is not a controversial subject. When we get specific, however, things change. For the longest time, Walmart was a controversial subject because many said that it put mom and pop shops out of business. Now, Amazon has become the retail villain. In addition, certain special interest political groups will often fight innovation since the process may hurt their position or cost the industry jobs. Unions have often fought against labor saving-innovation and some education groups try and prevent certain innovation in education.

For this program, we are not going to take a position on what is good innovation and what is bad. We are only going to talk about it as a factor and allow the participant to determine if he or she believes that the innovation is good or bad. However, we do have to address this pressure as something that will either promote or hinder the innovation depending on the power of any group. That pressure is very different in certain markets and depending on who might be affected by the innovation. To ignore it would be unfair to the complete understanding of what is occurring.

E. Some examples

1. Publishing

The publishing of books for the consumer market represented an archaic, complicated, and very inefficient system. There were several steps to the process with each step costing money and affording a profit for someone. Jeff Bezos came along and innovated how books would be published and distributed. Amazon was born, and it obviously disrupted the book publishing and selling market. Today there are very few brick and mortar bookstores, and the disruption is quickly moving to other methods. Once Amazon innovated books, it quickly expanded the concept to the point where it is now selling almost everything.

What markets have been disrupted with this innovation? Almost all retail. And yet, many physical retail locations refuse to recognize the disruption and are making attempts to hold on.

2. Taxi services

The innovation of taxi services to the point where Uber and Lyft have dominated the market and significantly disrupted traditional taxi service is interesting. What has happened is obvious, but we should analyze the why to discover a lot about disruptive innovation. Actually, the price is not the really important thing. Yes, many will find the Uber and Lyft to be a little less expensive, but most riders will discover that the service is more about convenience. The real innovation was the use of the cell phone in a totally new way that caused huge advantages of convenience for the consumer. It's easy to call the ride, easy to pay, generally find friendly on-time service, and have fewer problems in most areas.

This is also an interesting example of how often the established markets will attempt to fight innovation. When Uber first started, unions influenced cities, and the governments did everything they could to regulate the service out of business. However, as is often the case, when the public gets a taste of something better, it will demand it of the regulators.

We can learn a lot from this example. Most importantly, we can expect other things to be innovated through convenience through the cell phone. An example is food delivery services that use a phone app to order and have the food delivered. Is this more expensive? Yes, but far more convenient.

3. Hospitality

VRBO and Airbnb are institutions born out of convenience, price, and lack of regulations. When I want to take a family vacation, I will first look to see if there is a vacation rental available rather than going to a hotel. This is a great departure from the past over relatively few years, and our decision is primarily that we get more room for the same amount of money. If you were in the hotel business, would you consider that you had been disrupted? Certainly, as the vacation rental market has certainly eaten into the hotel market. To most people the value is better, and the convenience is little different. Are the hotels fighting the innovation? Certainly, through lobbying for regulation; however, in most cases they are relatively unsuccessful in denting the market.

What can we learn from this innovation? Probably it goes back to the concept of convenience of a transaction online or over the cell phone.

4. Car rental

All you have to do is to see what has happened to the rental car market over the past few years, and you will see an industry that is ripe for innovation. While the corporate market will be the last to change, we are already seeing an interesting innovation with Zipcar. This is a rental system where you have a card, go to an available parked car, use your card to get in, make your trip, drop off the car in the same place, and go away. You never have to talk with a person, and the price is very reasonable. While obviously, this disrupts the rental car market, it also has an effect on the automobile sale market since people living in cities where zip cars are available are finding that even owning a car is unnecessary.

5. Driverless vehicles

As a disruptive innovation, school is still out on the effect of driverless vehicles since the technology is still being proven; however, when it becomes useful, it is sure to disrupt several industries. As mentioned, Uber and Lyft have innovated and disrupted the taxi industry, but driverless cars will obviously disrupt Uber and Lyft. More importantly, the truck industry will be totally disrupted. Presently there are just over 1.5 million heavy and semi-truck drivers in the US, and obviously their jobs will be threatened with driverless vehicles. Will they pressure to slow the innovation? Naturally, however, eventually the innovation will happen.

6. Web-based video

The home TV industry has been an interesting one to watch as it has developed from three channels to CATV, to satellite, and now to streaming. Is this a true disruptive innovation or just a maturing of a present industry? We won't try and answer the question, but it is an interesting one to watch and to speculate what other innovations will occur as a result.

7. Blockchain and cryptocurrency

This particular innovation is probably one of the least understood and most difficult to easily explain. I once read an explanation that has stayed with me and helped me to understand the concept. Think of it as a huge, limitless Excel spreadsheet that anyone (with the proper password) can change. Consequently, if I want to send you money, all I have to do is to go onto the spreadsheet and credit your account. There are no middlemen, banks, financial institutions, or governments controlling the system.

The definition of money has traditionally been, "a medium of exchange or a store of value." Would the cybercurrency meet that definition? While the currency is the most often discussed aspect of this innovation, it can and will directly affect many other industries including title companies, law offices, governments with documents, and countless others. It will be possible to pass both money and documents directly from one party to another without having to go through an intermediary. Many industries will be disrupted from this innovation.

8. 3D printing

A few years ago, I went to my dentist for a crown. He prepared my tooth, made a mold with a horrible tasting piece of plastic, and told me to go home and not chew on it for a week while he sent the mold off to a lab to have the tooth made. Last week I went to the dentist at 10:30 AM and came home by noon with a new crown on which I didn't have to avoid chewing. What's the difference?

The answer is that the dentist prepped the tooth, scanned my mouth, and a 3D printer used a supply of porcelain and actually built the new crown from the digital specs from the scan. Was the process less expensive? No, since the dentist has to amortize the machine. The innovation will obviously change that aspect of dentistry, but more importantly, it may very well have a huge detrimental effect on dental labs.

9. Telemedicine

Just the other day I heard about a recent surgery that was performed remotely by a robot. This innovation, and similar ones like it have already impacted the health industry and they will continue to do so. It is, however, interesting to discuss the difference between dentistry and medicine. Obviously, they are similar; however, while dentistry is primarily a private pay situation, medicine is much more controlled by the insurance companies and Medicare. Consequently, we see differences in regulation and differences in what is permitted.

Many of us, especially those of us senior citizens, regularly see a doctor for routine conditions. In some cases, we do very little, if anything, with the doctor other than talk. Could this be performed over the phone, by email, or in some more efficient way? The answer obviously is yes; however, the slow-moving regulations of the insurance industry will have to exactly determine how much to charge and how to bill for such services. Will it happen? Absolutely yes, but it may be a while. I would predict that we will soon see some significant improvements in medical efficiency that will tend to curb the medical inflation that we are now seeing.

10. Artificial intelligence

Although AI is another area that could be referred to as more of a gradual innovation, it certainly should be considered here as we look for things that could cause our organization huge risk in the business model. I like to think of AI as intellectual robots – the computer is doing something that formerly was done by the human brain. As of right now I am using my brain to write program materials. In the coming years will this be able to be done by computer and all I will have to do is a little outlining? The areas which will be disrupted due to this development will be various ones that formerly took human thinking. That will probably include almost all kinds of decisions such as diagnosing a problem or sickness or making a decision on a loan. We used to think that the operating people were the ones that would be replaced by robots. Today, the management jobs and industries are at risk of being disrupted.

11. Education

I'm not sure of any industry more in danger of a huge change than education, and especially higher education. Already much education is being performed online, and this development will continue. Colleges and universities all over the world are developing classes made available at low cost to students over the Internet.

F. Which industries face the greatest strategy risk?

In a free-market economy, the theory is that innovation will take place as long as it is economically advantageous to do so. However, some parts of our economy are freer than others. The ones that are less free and more protected by regulation will be the slowest to innovate; whereas, the parts with fewer regulations and protections will innovate sooner.

1. Margins and profits

The old saying, "follow the money," is probably a correct concept. Industries in which costs of the products or services have increased the most are probably indicators where there might be an opportunity for greater efficiency with disruptive innovation. Higher education is a great example. The cost of the service has increased over the past years many times the rate of inflation. Why? There are many reasons, but there is no debate that it has happened. Consequently, there is more incentive to innovate and lower the costs. Southern New Hampshire State University, as well as others, has innovated by concentrating a huge effort in online education.

Another example of high margins and low efficiency is publishing. What used to be a multiple-step, archaic process has been vastly innovated into a much more efficient business model.

Often high sales costs will cause an industry to innovate to one with low sales costs. This is exactly what has happened with the advent of many, if not most mattresses being sold online, rather than in mattress and furniture stores.

There are two other industries that may be in a high-risk position of sales innovation due to high cost. I think that there is no question that someone is going to find a far more efficient way to retail automobiles. The trend is already starting with used cars, although it hasn't taken hold yet. I believe that in the next 10 years we will see a major innovation into the business model of retailing new cars.

The same thing is true of real estate. Traditionally, a 6 to 7% commission is paid by the seller; however, as home prices have increased, this amount is often seen as high. Presently, there are several innovative ways to sell homes using a more efficient model, and soon one or more will be accepted, and the industry will be innovated.

2. Highly regulated industry

Industries where there are a high number of regulations, but an innovator can discover a way to bypass many of the regulations with another business will often do so. This is the primary reason for Lyft and Uber. Due to the high regulations the traditional taxi companies were protected. Then, Uber and later Lyft found ways to get around those regulations and lower the cost to the consumer. Airbnb and VRBO could also be examples of this.

3. Disintermediation

This is a long word that essentially means to cut out the "middleman." Primarily, it has been the Internet that has enabled this concept. Once a manufacturer sold through distributors who sold through retailers to the customer. Now, in some cases, the manufacturer will sell directly to the retailer thus cutting out (disintermediating) the wholesaler, or in some cases it will sell directly to the consumer thus eliminating or disintermediating two steps. The key here is to ask yourself, are we a "middleman"? Are we at risk of being cut out?

4. Hierarchal vs people led

This is an important concept that is often not seen. Over the past several years we have been moving through a process where more hierarchal top-down companies have been replaced by more populous type organizations. The best example is Wikipedia. Once there were several large encyclopedia companies with teams of editors who were the ones to decide on what is considered truth. If you read it in the Encyclopedia Britannica, then it was considered truth. The editors made that distinction. Today, Wikipedia has a totally different concept about who should determine truth. That organization believes that it should be determined by the public with people correcting each other until there is agreement on truth.

When it was first started it was distrusted by the more established institutions such as schools. Now, many are accepting that the system works and is much more able to get current information into the hands of the public.

G. How to approach business model risk

1. Defensive

Following this strategy will have you develop a plan to defend your business model. If you are a retail store recognizing the innovation in online retail, you will need to determine what advantages your model brings customers and exploit those to the point where the innovation will have no effect on you. If you are an intermediary, you have to be sure to add value at your level to make sure that your customers will not want to go around you even at a lower cost.

Finally, be sure not to allow your internal politics to put the organization into a state of denial as happened at Kodak and many other large organizations. Recognize the risk early and institute a strategy to combat against it.

2. Offensive

The offensive approach is either to be the innovator where you see an opportunity or at least get on the innovation early when you see it develop. This approach will usually be seen as a higher-risk strategy; however, it can also have very high rewards. For this approach, you will need a very active R&D program and make sure that change is at the top of everyone's mind.

3. Covid-19

Without question, the recent pandemic either caused or accelerated business model changes. While education had been moving to an on-line model even before the pandemic, it has now become required. Retail has been heading to the Web, but that change was also accelerated. Now, you can even purchase an automobile without ever visiting the dealership.

How has this affected your organization?

IV. Reputation risk

In the above-mentioned Deloitte study, reputation risk was discussed as the number one strategy risk facing the company today. Probably this is because so many companies have been damaged by news stories and social media activity hurting the brand. The current availability of digital information has certainly put this risk into the forefront.

Damages to the brand can strike without warning completely shifting the corporate landscape by weaving negative content into the search results of the organization. Most risk management represents risks that are predictable and consequently being somewhat managed. Unfortunately, occurrences that damage the brand are mostly unpredictable. But they are certainly serious.

There are numerous types of risk to guard against including outside events, workplace practices, data breaches, product recalls, bad financial condition, and management reputation issues. All of these, and similar items, are the responsibility of senior management and the board.

A. Measure

Do you know the reputation of your company? You might ask, among which group? The answer is: all of them. You should know the reputation of your company among each stakeholder group including customers, employees, investors, suppliers, and community. The best, and easiest way to accomplish this is to establish a system of surveys among the groups. Using inexpensive tools such as “Survey Monkey,” you can easily measure your reputation.

The key is how to word the questions and what to do with the information. First, have a simple survey with very few questions. You know that we are all deluged with surveys, and most of us won’t respond to most of them. But, why do many companies pursue the strategy? Because it works for them. The most important thing is to keep the survey exactly the same and continue to survey over time. Consequently, it isn’t the number you are looking for it’s the trend. You want to see your reputation going up among all groups and you see this by watching the trends and not the individual numbers. To accomplish this, you have to use the same questions and do the survey frequently.

B. Manage

1. Have a social media strategy

Without question, every organization must have an official social media strategy, and that strategy should NOT be how to keep your employees off Facebook. Social media can, and should be, your friend. It is one of the greatest ways to communicate with the outside world, market, and otherwise build your brand in a positive way.

2. Communicate

Many reputation problems occur because a small problem got larger. In some cultures, being candid and admitting mistakes is not frequent. Consequently, there is a tendency to hide mistakes and hope that they go away. For example, a customer gets into a disagreement with a customer service person. That kind of occurrence is obviously frequent, but this time the customer was a minority member and decided to make an issue of it. Senior management never knew about the problem in the first place and didn't find out until the local TV station called and wanted a comment before airing the story of your company's discrimination lawsuit. The reputation risk may not have been avoided, but it sure would have been nice if senior management had known about the problem sooner.

3. Customer service issues

This is a very difficult area to discuss from the standpoint of organization reputation. We have standards, policies, and try to do the right thing. That's why, when a customer attempts to steal from us and force us to violate those policies, we often stand on principle. The problem is that kind of firm stance can be expensive. When we get into a dispute with a customer, especially over a relatively small amount of money, it is often far less risky to give in rather than stand on our policies. Even when the organization is clearly right and the customer wrong, we should generally recognize the potential risk, and quickly give the customer their money back.

C. Mitigate

The most important aspect of mitigating the reputation risk is to have a well-conceived plan. We should have a specific plan for social media, including all of its branches like Factbook, Twitter, Instagram, etc. Our positive plan should be built around how we can improve our brand and reputation. In addition, it should include a way to carefully monitor what is being said about us.

Part of our plan should also include going through a complete "what if" analysis regarding customers. Generally, this plan should include empowering and training low level people in how to avoid and quickly defuse problems at the customer service level. Customers do not want to hear something like, "I would love to give you your money back but it's beyond my authority."

Training is by far the most important type of mitigation. After all of the cases of reputation risk that we see in the news, it's amazing how many organizations get hurt because an employee said or did something stupid. More importantly, often it is senior management. How often do we see how the tweet of a CEO or an email becomes public that contains embarrassing information or words? The most important part of the training has to be, "Never ever say anything for which you or the organization might be embarrassed." We think that things like messages and email are private communication and won't be seen by the public. No, we have to assume that EVERYTHING we say will become public. If we don't want people to know what we say, then we shouldn't say it!

D. Monitor

This is a subject for the IT people, and possibly beyond the scope of this program, but we need to discuss that it be done, and not how to accomplish it. Fortunately, through tools like Google Alerts, we can have computers carefully monitor what is being said about our organization. We obviously need to be using these tools since with the information we can develop our plans.

V. Manpower risk

While this could be an entirely separate risk if we go into all of the details, for this program we will consider it part of strategy risk since we will deal with only the strategic aspects of the risk and not the operating risks.

A. Culture

In a previous chapter we discussed the aspect of the culture of the organization and its effect on risk. We need to again examine it from the standpoint of manpower risk. The culture of the organization will be determined by the employees with the greatest emphasis from the top. If the CEO wishes to operate in a certain culture, most likely the organization will adopt that culture. Consequently, since culture affects risk, it's important to have a strategy for the desired culture. It's very important to look at the culture and determine if any changes are desired. Since generally the team culture produces the most successful organizations, many companies will choose to attempt to move in that direction.

B. Turnover

Employee turnover costs money when hiring and training costs are factored into the equation. Consequently, having a plan to reduce turnover will generally result in lower turnover, a better culture, and lower risk in this area. From a financial standpoint, it's important to carefully calculate issues of turnover and employment cost factoring in those other areas. In my opinion, too many organizations look only at the costs of salaries and fringe benefits without looking at the other factors.

C. Morale

Employee morale can be measured in several ways, but the employment engagement survey is considered to be one of the best. Experts report that when employees are engaged with their work, they're more fulfilled and more motivated. That ultimately leads to higher productivity. Consequently, the cost of the survey is almost always well covered by productivity costs.

1. Survey often

It's important to survey the employees often and with the exact same questions. The reason is that the results can be tracked on a graph and the organization can see how the strategy is doing.

2. Have a plan

Having a survey without a plan to improve the metric is a waste of time. In fact, often the employees will see the absence of a plan of improvement, and the result will be lower morale.

D. Productivity

Simply stated, productivity is the ratio between inputs and outputs. If the inputs include manpower costs, then the amount that the people can produce will affect the cost of the product or service. Therefore, what we can do strategically about productivity will affect the output costs. Culture, morale, and turnover will affect productivity.

E. Integrity

If an organization has employees without integrity, the risks will be much greater. Those employees who have better morale and more engagement will generally show greater integrity and be less apt to make decisions that put the organization in undue risk.

F. Managing manpower risk

1. Pre-employment screening

Before we take employees into our organization, we must interview them carefully to make sure that they will fit into our culture. While we don’t have the time to discuss all the details about interviewing, if we want the best employees who will give us the lowest chance for negative risks, we need to hire people with the best attitudes in addition to having good skills. Organizations who make hiring decisions based only on skills without sufficient attention to attitude will end up with highly skilled employees with low engagement, low morale, and high turnover. Most importantly, the culture will be negatively affected.

2. Performance evaluations

In the same way, we must evaluate our employees on the basis of their attitudes, ability to get along with the team, and other “soft” skills as well as the technical skills.

3. Chemical abuse

Employees who abuse alcohol and other drugs can add to the risk of the organization in many ways. Consequently, for a good risk management program you absolutely must have a program to detect and mitigate chemical abuse.

4. Payroll controls

Along with all of the internal controls of the organization that help to lower the fraud risk, payroll controls are extremely important and part of manpower risk.

5. Key person loss

Most organizations will have a plan in place to lower the risk of losing one or more of the key leaders. Such a loss obviously represents a major risk. This should be done both by lowering the risk of the loss and also making sure the organization has a backup should the loss occur.