5 Steps Towards an Actionable Risk Appetite
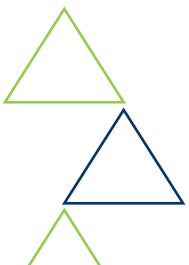
Introduction

Risk appetites and tolerances are an integral part of any successful business. Why is that? Because every day, personnel ranging from front-line employees all the way to the board of directors are making decisions that greatly impact the business. As a governance professional, it's your job to make sure these decisions are directly in line with the company's unique goals and objectives.

Risk appetites and tolerances are the perfect way to make data-driven, performance-enhancing decisions, while developing a system to understand when and where your business is taking on too much risk, or not taking on enough.

In this eBook, will explore the difference between risk appetites and risk tolerances, as well as 5 major steps you can take to make sure these statements are actively propelling your business towards a better tomorrow.

Table of Contents

Chapter 1

Understanding Risk Appetite and Risk Tolerance

An organization-wide risk appetite can be a powerful statement that gives your risk program direction. However, like any policy, risk appetite without accompanying action is nothing more than an idea.

So how do you make risk appetite actionable? The answer is to implement risk tolerances.
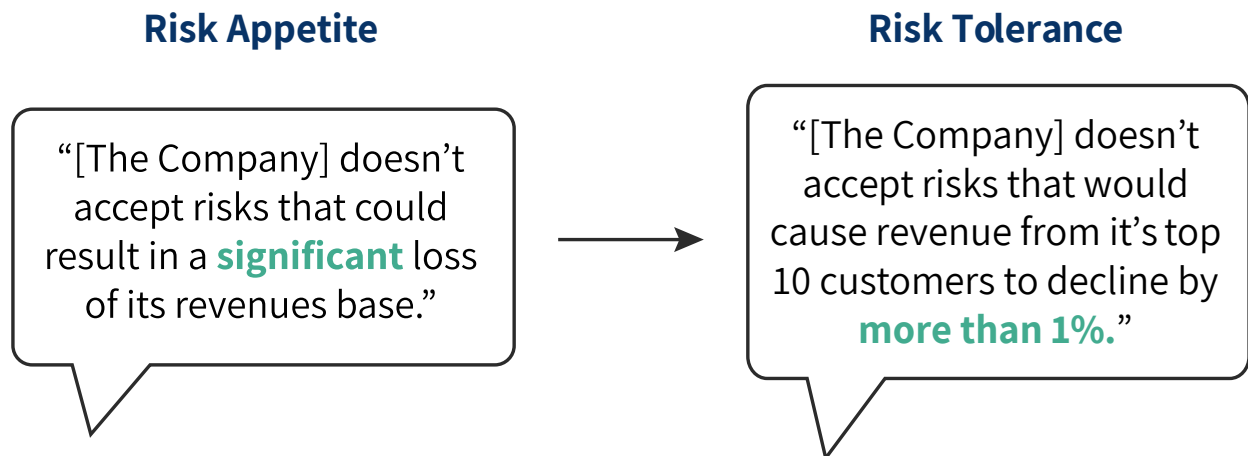
Defining Risk Appetite and Risk Tolerance

According to the IIA, both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept, but there is an important difference between risk appetite and risk tolerance. Understanding this difference is crucial for developing an effective risk program that actually helps your company's performance, as well as tracking its effectiveness over time.

Risk Appetite vs. Risk Tolerance

Risk appetite is a higher-level statement that considers the broad levels of risk that management deems acceptable. A risk appetite statement sets a course of action, or goal, based on what the organization would like to achieve. Risk tolerances, on the other hand, set acceptable levels of variation in performance that can be readily measured.

For example, a company that says it doesn't accept risks that could result in a significant loss of its revenues base is expressing a risk appetite. When the same company says it doesn't wish to accept risks that would cause revenue from its top customers to decline by more than a fixed percentage, it is expressing a risk tolerance.

Risk Appetite

"[The Company] doesn't accept risks that could result in a **significant** loss of its revenues base."

→

Risk Tolerance

"[The Company] doesn't accept risks that would cause revenue from it's top 10 customers to decline by **more than 1%.**"

Examples of Risk Appetite and Risk Tolerance

Here are a few more examples of risk appetite and risk tolerance statements.

Our first example looks at a health service organization. This organization's risk appetite, as you can see, is a high-level statement that simply sets standards on where they're willing to accept risks. Their risk tolerance statement is much more granular, going as far as to set levels of acceptable patient wait-times.

Risk Appetite	Risk Tolerance
Treat 85% of patients within the industry standard of acceptable wait times.	ER patients must be treated within 90 minutes of admission, and critically ill patients within 10 minutes. No less than 95% of non-life-threatening injuries must receive attention within 3 hours of admission.

In our second example, we're looking at a company in the finance industry. For a risk appetite, management has decided it is willing to accept small losses in 15% of investments it has deemed 'risky.' Again, this risk appetite is more high-level and less granular than the risk tolerance, which states the company can't lose more than 75% in over 5% of its investments, along with not losing more than 25% in over 30% of its investments.
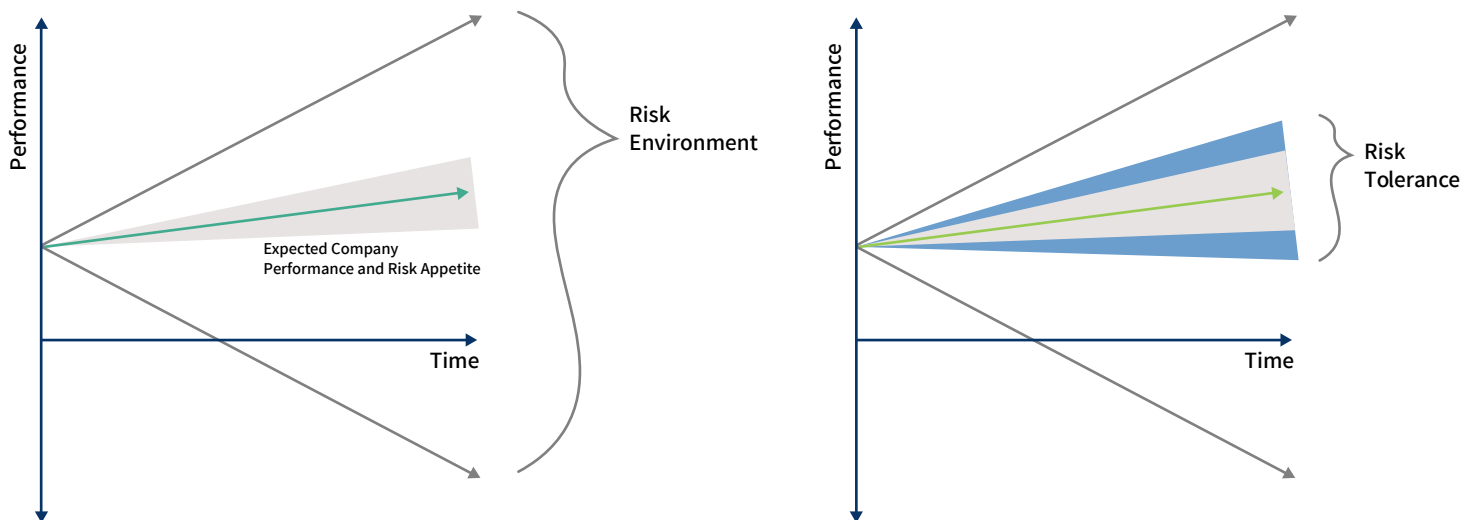
| Risk Appetite	Risk Tolerance
The firm is willing to accept small losses in 15% of its "risky" investments.	Don't loose more than 75% in over 5% of investments, and don't lose over 25% in more than 30% of investments.

Examples of Risk Appetite and Risk Tolerance

Let's look at a graphic representation of risk appetite and risk tolerance. In the charts below, the organization's projected path of performance is plotted in green. This line and the immediate area around it represents the risk appetite, or goal of the organization. If the organization was to pursue or retain all risks in their environment, their performance could fall anywhere between the grey lines. Most organizations are uncomfortable taking on all available risk, and new laws and regulations require companies to implement more narrow tolerances, which is highlighted in blue.

Operating within risk tolerances provides management greater assurance that the company remains within its risk appetite, which in turn, provides a higher degree of comfort that the company will achieve its strategic objectives.

Before we leave the subject of actionable risk appetites, we'd like to show you another way to leverage risk tolerance statements. First, you can use your risk tolerance level as a "cut level" to better determine which risks require more resources and attention.
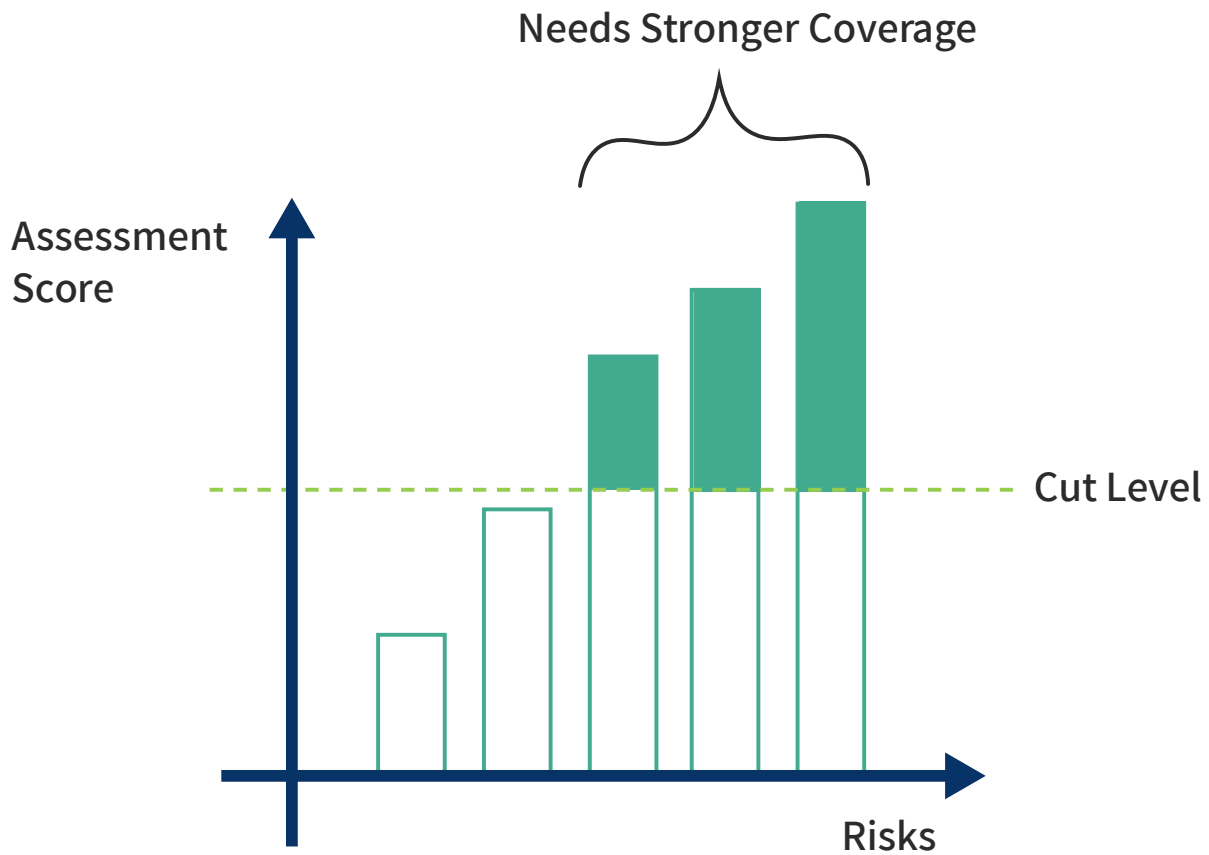
Conducting a gap analysis with a risk tolerance level will help you identify emerging risks before they rise out of tolerance and it becomes clear that certain mitigation activities are no longer sufficient. Everyday, process owners are making operational decisions about risks without reading their organization's risk appetite statements. This means that process owners must evaluate their assessments and, if a risk exceeds a set tolerance, adjust mitigation activities, procedures, or controls to get within the tolerance.

Over time, risk tolerances will align overall risk appetite and strategic goals, improve risk mitigation effectiveness, and allow you to achieve your strategic goals. Aligning your tolerances with risk appetite and strategic goals can be challenging, but trending risks over time allows you to get a more accurate picture of where you are and where you need to be.

Chapter 2

5 Steps Towards an Actionable Risk Appetite

There is a lot that goes into the formation, implementation, and monitoring of risk appetites and tolerances. To simplify the process, and make it as applicable as possible, we have outlined the five most important things to consider when putting risk tolerances into action.

Step 1. Align Tolerances with Strategic Goals

Your organization's goals can be categorized in many ways. To create an actionable risk tolerance, we divide organizational goals and risk tolerance into 3 areas with a top-down approach:
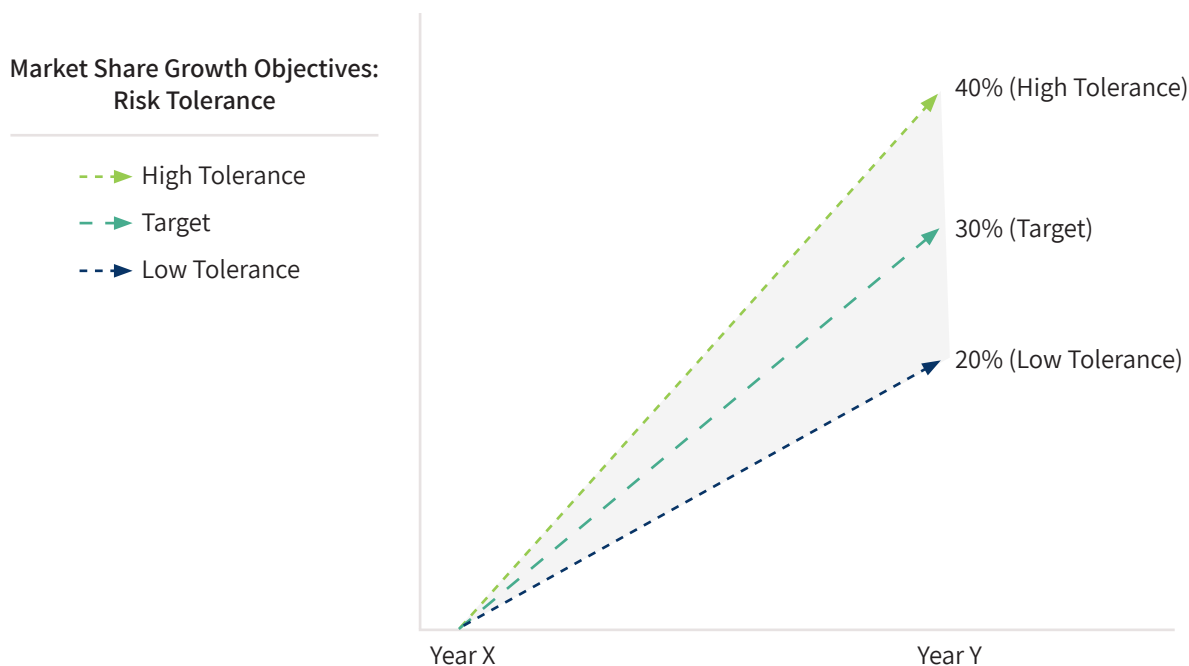
- Strategic
- Tactical
- Operational

Consider this very simplified example on how to create an actionable risk tolerance at the strategic level:

Start from the top with your strategic goals and create a risk appetite statement as it relates to those goals. Here we see a risk appetite statement relating to a company's goals for market share growth. The statement is general and discusses the type of risk an organization is prepared to pursue:

"[The Company] will take risk in the pursuit of strategic success, but only if those risks align with strategies to meet market share growth objectives by the end of Y year."

This is a high-level strategic goal – a vision of where management sees the company down the road. From here, we can move on to an associated tolerance range. In this case, the target for market share is 30% by the end of Y year, with a tolerance that ranges from 20% to 40%.

At this point, our risk appetite statement is linked to strategic goals. Achievement of these goals will ensure the organization is within its risk tolerance.

Market Share Growth Objectives: Risk Tolerance

- - -► High Tolerance
- — ► Target
- - -► Low Tolerance

40% (High Tolerance)

30% (Target)

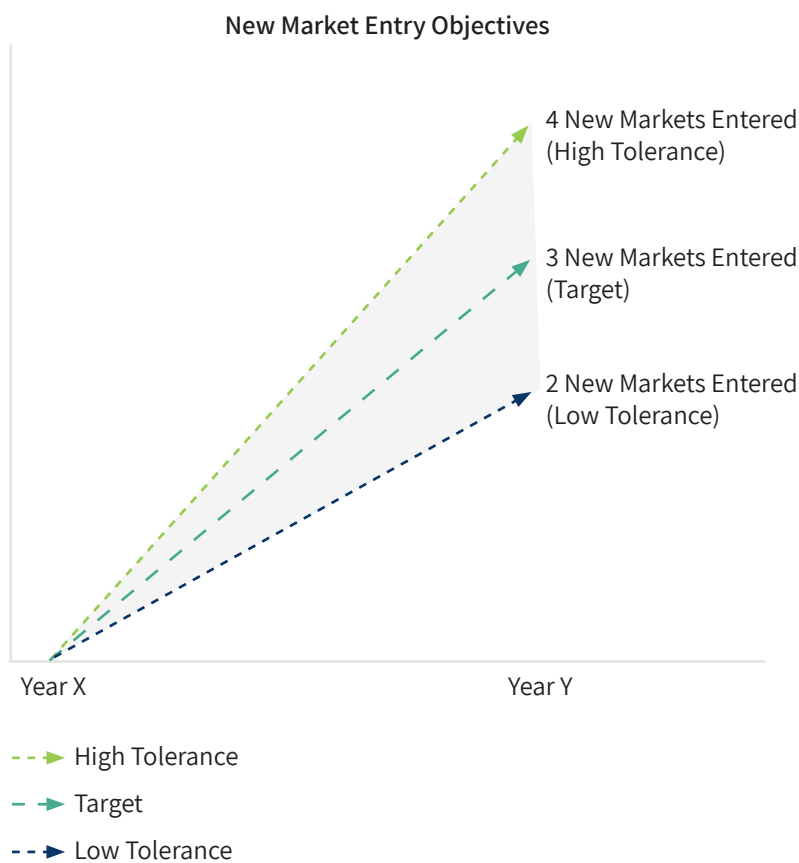20% (Low Tolerance)

Year X   Year Y

Step 2. Translate Risk Appetite to the Process Level

Every day, throughout every organization, front-line managers make operational decisions involving risk. These lower-level management decisions can be the most frequent, as well as most impactful, decisions made within a company. Implementing risk tolerances at this level is vital. By doing so, you are connecting front-line decisions with the organization's overall goals and risk appetite. This process begins by translating strategic goals to the tactical level.

Tactical goals describe high-level activities which facilitate the achievement of strategic goals. In this case, the strategic goal is to increase US market share to 30%. At the tactical level, the company will accept risks that align with these strategic goals, specifically related to new market entry. In this case, the company aims to enter 3 new markets, with a tolerance range of 2 to 4. This represents a risk tolerance at the tactical level, closely linked to strategic objectives:

"[The Company] will take risks in the pursuit of strategic and tactical goals, only if those risks align with the tactical objective to expand US market presence during Y year."

New Market Entry Objectives

4 New Markets Entered (High Tolerance)

3 New Markets Entered (Target)

2 New Markets Entered (Low Tolerance)

Year X — Year Y

- - ▸ High Tolerance
- - ▸ Target
- - ▸ Low Tolerance

At this stage, companies should think about leveraging tradeoffs in tactical activity. For example, while The Company expands to new US markets, it might choose to reduce focus on European or other international markets to free up resources for this expansion.

By formalizing tolerances, risk managers clearly communicate a risk/reward tradeoff. Now, leadership isn't caught off guard if negative events occur in the interest of these larger corporate goals. Effective risk management should result in efficient use of the company's limited resources, leveraging new opportunities and driving increased enterprise value.

Now, we take it to the operational level. This level covers short-term, specific goals that facilitate tactical and strategic objectives. By looking at operational activities within the organization, we can determine goals as well as associated control activities and risk tolerances. In this case, the company is willing to take risks that align with both strategic and tactical objectives. The Company focuses on specific operational activities which will allow these goals to be achieved:

"[The Company] will take risks in the pursuit of strategic, tactical, and operational goals, but only if those risks align with operational objectives for employee hiring and training, and efficiency in operations."
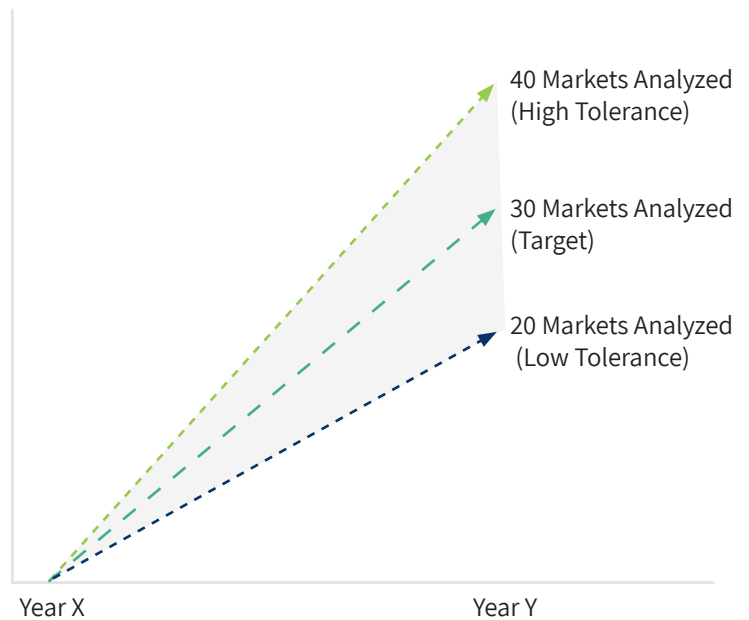
Managers then create tolerances around these operational goals, in this case around staffing and performing market analyses. Since these operational goals are tied in closely to tactical and strategic goals, managing activity at the operational level ensures achievement of strategic goals. This is the benefit of "translating risk appetite to the process level. This process relies on engagement from managers in each level of the company.

Marketing Department Staffing Objectives - Risk Tolerance

8 New Hires
(High Tolerance)

6 New Hires (Target)

4 New Hires
(Low Tolerance)

Year X   Year Y
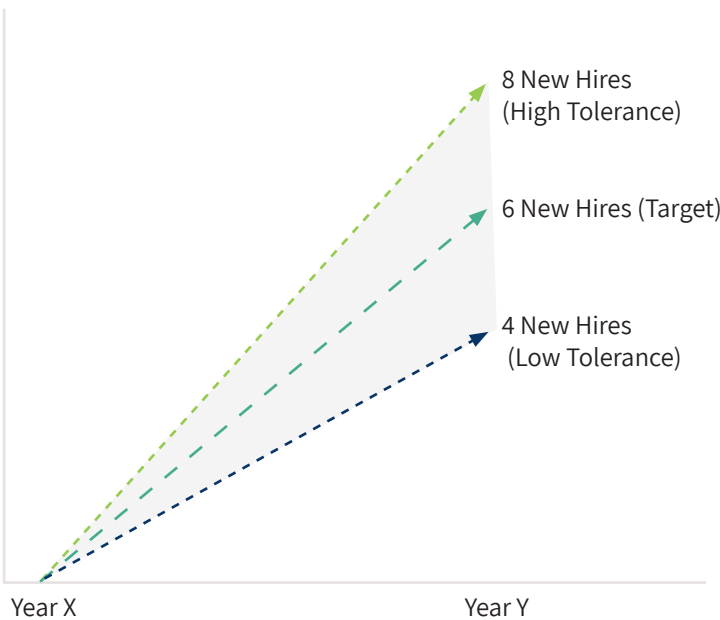
- - ▶ High Tolerance
- ▶ Target
- - ▶ Low Tolerance

Marketing Department Operational Efficiency Objectives - Risk Tolerance

40 Markets Analyzed
(High Tolerance)

30 Markets Analyzed
(Target)

20 Markets Analyzed
(Low Tolerance)

Year X   Year Y

- - ▶ High Tolerance
- ▶ Target
- - ▶ Low Tolerance

The example covers very high-level activities. In initial assessments, operational activities can be as granular or as high-level as is appropriate to demonstrate value to your board or senior leadership. By linking to higher-level operational activities, you can easily establish relationships between general business process areas and strategic risk tolerances. By identifying more granular activities, you can begin to gain tighter control and more oversight over your risk levels relating to strategic risk appetite and tolerance. Both of these approaches lead to better business decision making as a result of your ERM program.
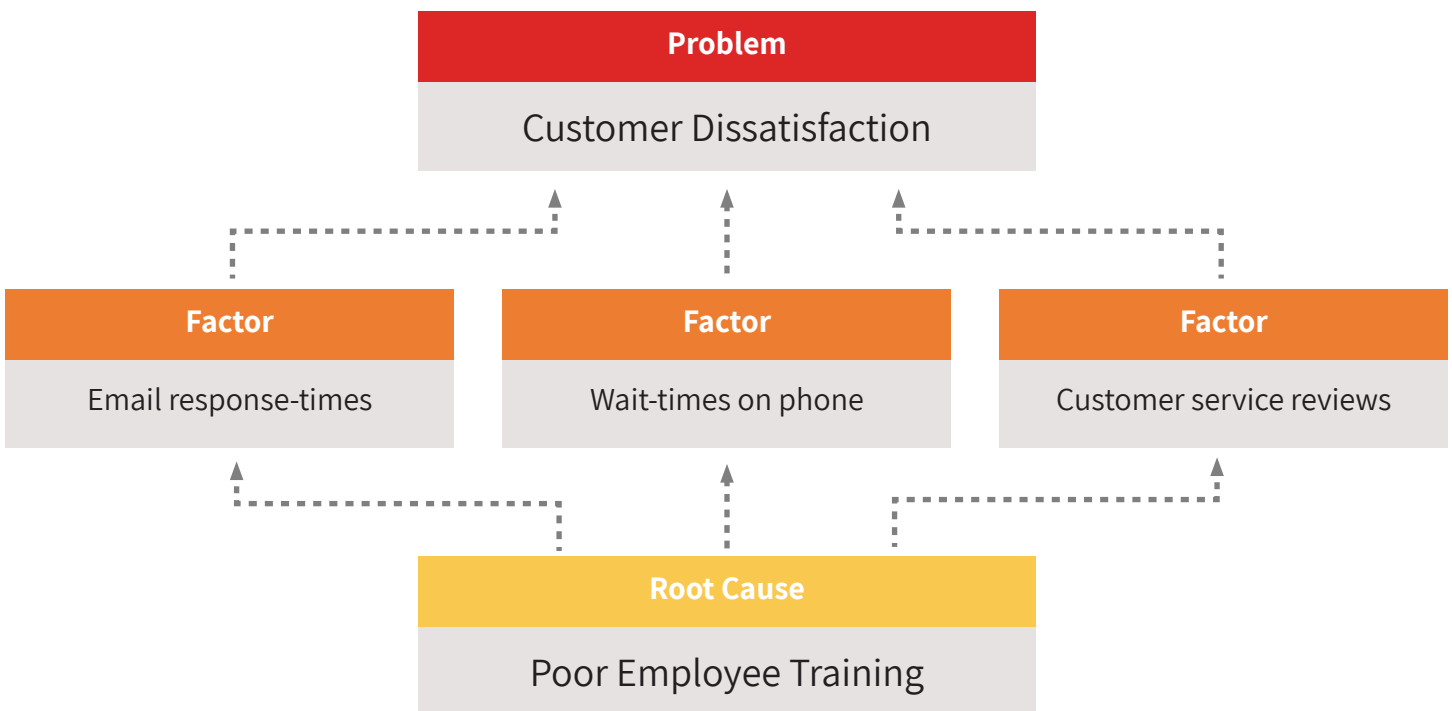
Step 3. Set Risk Tolerances Around Root-Cause Analysis

Once risk tolerances are established around front-line processes, you then need to decide on the appropriate metrics to track and measure success. To do this, you need to be monitoring the root causes of risk at every level.

For example, say your risk appetite sets a low tolerance for customer dissatisfaction. Here, a logical metric to track would be customer satisfaction levels over time. You might choose to implement customer surveys to measure these levels. Methods like these, however, fail to address the heart of the problem. No matter what the survey results say, you are only measuring satisfaction against predetermined dimensions. You're still missing ways to catch unidentified root causes of the problem, which could bring about actionable solutions for raising customer satisfaction.

Instead, it is best to track the specific root causes of customer dissatisfaction. Looking at factors like call wait-time and email response-time provides insight that can be acted upon, allowing you to adapt business processes and meet organizational goals. While these factors contribute to the high level of customer dissatisfaction, they are not the root causes of the problem. Through risk assessments, all three factors can be traced back to one central issue: poor employee training. Once a root-cause risk is identified, mitigation activities and controls are put in place, and the organization works to improve business processes and eliminate the associated problem.

Problem		
Customer Dissatisfaction		

Factor	**Factor**	**Factor**
Email response-times	Wait-times on phone	Customer service reviews

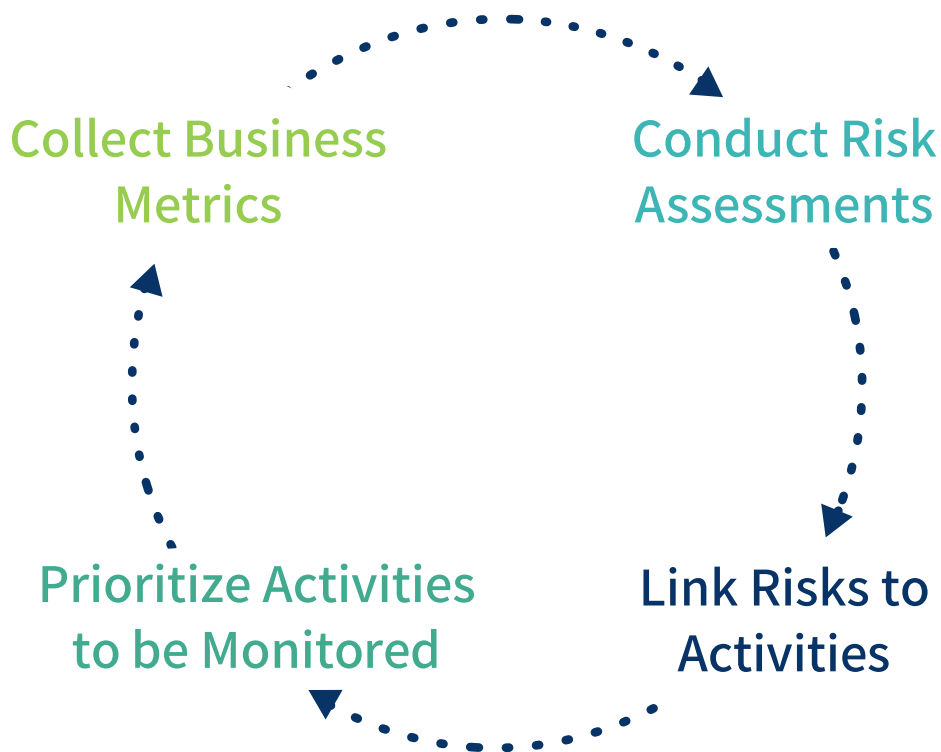| **Root Cause** |
| --- |
| Poor Employee Training |

Step 4. Collect Forward-Looking Risk Metrics

Another roadblock in being able to apply risk tolerances in an actionable way comes from the way current risk mitigation activities are collected and reported. Typically, metrics collected around risk only measure what has happened to date, and do not provide many insights into recurring patterns that could affect your tolerances. Establishing more forward-looking points of reporting will allow you to detect emerging trends long before they have significantly impacted your organization.

Let's go back to our example of wanting to increase customer satisfaction. Avoid using tools like surveys and yes-or-no testing for monitoring mitigation activities, such as how often employees have customers on hold for 2 or more minutes. These types of collection methods only test compliance with internal policies, which may or may not tie back to the specific risks that the policies were designed to mitigate.

When tracking an identified root cause of a problem, like unsatisfactory employee training, make sure you're measuring it in the right way. Tracking counts of complaints against employees alone is not comparable over time or across products because the number of total customers will always vary. Instead, measure and compare root causes in percentages. For example, compare the percent of customers who complain after interacting with employees who completed an advanced training program to those who only completed an older, less comprehensive, training program.

This will be a more meaningful metric as its value is independent of customer volume and is thus comparable both over-time and across silos. As always, visualize your data to understand the root causes of why problems occur and take preventive action.

Collect Business Metrics

Conduct Risk Assessments

Prioritize Activities to be Monitored

Link Risks to Activities

To help make choosing the right metrics easier, employ a risk-based balanced scorecard approach for identifying the correct root causes of risk. A balanced scorecard is a management system that enables organizations to clarify their vision and strategy, and then translate it into action. It provides feedback around both the internal business processes and external outcomes in order to make sure you are continuously improving strategic performance and results at every level. When fully deployed, the balanced scorecard transforms strategic planning from an academic exercise into the nerve center of your enterprise.

Each of the 4 areas in the balanced scorecard look at how your internal operations are affecting external outcomes by defining the appropriate objects, measures, targets, and initiatives for each.

For example, when evaluating activities categorized under the internal business processes area, you go from looking at all processes within your organization to those that are actually adding value for your shareholders and customers. You can then create mitigation plans that ensure the continued performance of the processes that produce the most benefits, and improve those that are underperforming.

The balanced scorecard approach also provides you with a way to identify non-value added activities within your organization. This makes increasing the efficiency of your organization easy by providing a lens for seeing where to streamline repetitive activities and where to remove unnecessary steps in your business model.

The Risk-Based Balanced Scorecard

Customer

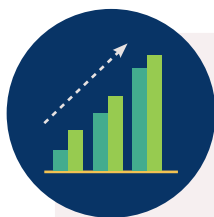To achieve our vision, how should we appear to our customers?

- Objectives
- Measures
- Targets
- Initiative

Financial

To succeed financially, how should we appear to our shareholders?

- Objectives
- Measures
- Targets
- Initiative

Internal Business Processes

To satisfy our shareholders and customers, what business processes must we excel at?

- Objectives
- Measures
- Targets
- Initiative

Learning and Growth

To achieve our vision, how will we sustain our ability to change and improve?

- Objectives
- Measures
- Targets
- Initiative

Step 5. Align Your Risk Metrics Enterprise Wide

By aligning risk metrics on an enterprise-wide level, decision makers get a more holistic picture of what is happening in your organization and can determine goals for "what needs to happen" based on the most influential performance indicators across silos.

Accordingly, to go back to our first step, be sure to collect information around the three levels of risk appetite (strategic, tactical, and operational) for each of the 4 areas covered under the business scorecard.

Unfortunately, most organizations have no way of knowing how and if changes in these dimensions will affect their risk metrics. Typically performance management is done on spreadsheets, where the information needed to generate reports is scattered throughout multiple silos and levels. This prevents insight into the impact of emerging risks on goals that could blindside the strategic plans of the organization.

Risk-based scorecards and taxonomies alleviate this problem by not only letting you see risks out of tolerance in each area, but also how these risks relate to each other across silos. Making risk assessments with standardized criteria for impact, likelihood, and assurance will give organizations an objective view across business areas of which risks are most critical as they relate to strategic goals.

After risk assessments are completed, process owners must evaluate results. If a risk level lies above or below tolerance, managers must adjust mitigation activities, procedures, or controls to correct the issue.

Risk tolerance monitoring should result in a consistent program across business areas, and lead to a standard which is commonly understood relating to risk appetite and tolerance throughout the business. Testing of mitigation and control activities will be in place to ensure the effectiveness of the ERM program.

Over time, risk appetite and tolerance will evolve as your ERM program matures. By making these measures actionable from day one, you set the foundation for enhancements over time. As your program grows to become more integrated into all business functions, your tolerances can become more specific as you learn how your business risks affect strategic goals.

Collect Meaningful Metrics

Download a free copy of our eBook **"Meaningful Metrics: Using ERM to Inform Strategy"** to learn more about measuring the effectiveness of your governance programs.

Chapter 3

The Benefits of an Actionable Risk Appetite

There are countless advantages to using these five steps and implementing an actionable risk appetite and tolerance within your organization. However, because this process requires cooperation and buy-in from all levels of the organization, it might be helpful to give you more information on what benefits you can gain from following the five steps above.

Advantages of Risk Appetites and Tolerances

When it comes to risk appetite, the board of directors and management each play a pivotal role. Management's primary task is to develop the risk appetite, along with the associated practices and controls.

Then, it becomes the board's responsibility to oversee the risk management practices, making sure that they adhere to the established risk appetites and are implemented effectively.

Together, management and the board are each responsible for utilizing risk appetite, along with the entire ERM process, in a way to achieve the organization's strategic and tactical goals.

Considering how much buy-in risk appetites and tolerances require, what are some of the motivating advantages of implementing them?

For an organization, there are countless reasons to implement and follow a risk appetite statement. The most obvious include the ability to:

Articulate Acceptable Risks	Quantify Risks
Strengthen Controls	Resolve Tension in the Business Strategy
Endure Budgeting Accuracy	Align Incentives

This list of improved business processes highlights just a few of the wide-reaching, cross-functional advantages that an actionable appetite and tolerance bring to an organization.

Benefits of an Actionable Risk Appetite

As we've said, having a risk appetite defined isn't enough to reap its advantages. It needs to be actionable.

Creating an actionable risk tolerance enables the organization to function inside an effective enterprise risk management framework and take a risk-based approach to ERM.

Taking a risk-based approach means that all business activities and functional areas are implemented with a focus on risk management. This allows the business to manage risk and take advantage of efficiencies across business units. With this approach, each operational activity is tied to a high-level goal, making the management of risk tolerance and appetite easy.

Less risk of business continuity failure.

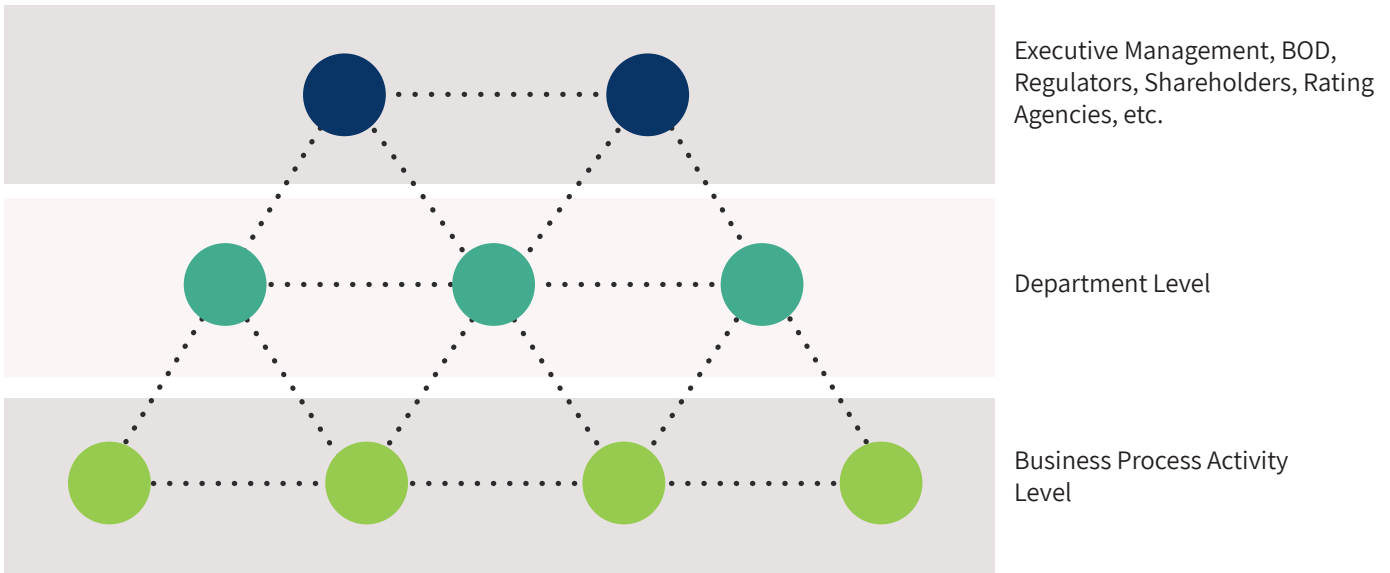Reduced time spent on risk management.

Improved data analysis, reporting and decision making across business areas.

Increased efficiency through resources focus on critical areas.

Greater understanding of how risks affect strategic goals and objectives.

However, it is difficult for most businesses to implement such a solution. Excel spreadsheets and PowerPoint presentations can only do so much. They do not function as an interactive, collaborative medium for ERM. This makes most ad-hoc solutions labor-intensive, error-prone, and inefficient. Effective ERM programs depend on the ability of managers and business process owners to receive important information from across the organization in a timely manner.

Executive Management, BOD, Regulators, Shareholders, Rating Agencies, etc.

Department Level

Business Process Activity Level

With perseverance, evidence, and a little luck, you'll be able to get the support you need from these three tiers of your business so you can be on your way to making data-driven, performance-enhancing decisions based on actionable risk appetites and tolerances.

Presenting ERM to the Board

Download our eBook **"Presenting ERM to the Board"** for more tips on how to deliver engaging reports to the board on your governance areas.

Build an ERM Program with LogicManager

You can get the most value out of your risk appetites with a centralized repository, automatic tasks, and automated reporting. LogicManager's ERM software can help you seamlessly implement these features into your new or existing risk management program.

Since 2005, LogicManager has empowered organizations of all industries and sizes to anticipate what's ahead, protect their reputation, and improve performance with strong governance.

REQUEST A DEMO

AUDIT
MANAGEMENT

BUSINESS
CONTINUITY & DR

COMPLIANCE
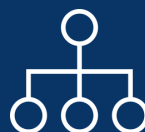MANAGEMENT

INCIDENT
MANAGEMENT

ENTERPRISE RISK
MANAGEMENT

FINANCIAL
REPORTING (SOX, MAR)

POLICY
MANAGEMENT

VENDOR
MANAGEMENT

IT GOVERNANCE
& SECURITY