LogicManager

5 Characteristics of the Best ERM Programs

+1 617 530 1210 | logicmanager.com | info@logicmanager.com

Introduction

A report by Forrester Research states, “Managing risk is more important than it’s ever been.” Risk management is surely a relatively new discipline, but what makes having a risk management program so important now?

We’ve taken note of an irreversible trend becoming more pervasive every day. We call this trend the **See-Through Economy**: a fast-paced age of transparency where consumers are empowered to impact a company’s reputation. The increasing adoption of social media and advanced technologies have granted consumers multiple platforms to express their expectations of the companies they choose to do business with.

With these platforms in the palm of their hands, consumers are empowered to record and disseminate any message they want, from a good customer experience, to a horrible one. The bottom line is that the general public has the power to influence reputation, buyers, investors, and regulators -- the major constituents of a company’s success.

The See-Through Economy has left companies with nowhere to hide when scandals, missteps, and failures materialize. This means reactionary measures are no longer enough to preserve a company’s reputation. Rather, companies need to take a proactive approach to managing risk before it materializes.

In this eBook, we’ll cover the 5 characteristics that add up to just that -- a proactive, integrated approach to managing a wide array of risk, otherwise known as enterprise risk management.

Table of Contents

A Shared Risk Culture and Governance Structure

Since 2008, Boards of Directors have been held accountable for the material impacts of a risk. This means the Board must be aware of the risks stemming from every level of the organization, even the front-lines. As a result, today's Boards are given a choice between having effective risk management, or disclosing their ineffectiveness in risk management to the public. According to the **Security and Exchange Commissions Proxy Disclosure Enhancements**, it is considered fraud or negligence if they do neither.

With liability for error so high, the Securities and Exchange Commission (SEC), the Institute of Internal Auditors (IIA), the National Association of Insurance Commissioners (NAIC), and Congress require increased accountability for risk management and a formalized ERM program. With all these regulatory changes, successful organizations are adopting a uniform risk culture and governance structure in order to promote risk-based decision making at all levels.

Three Lines of Defense

For any organization, risk is an essential part of creating business value, and as such it needs to be managed in a way that is beneficial to bottom line performance.

A risk governance structure needs to be put in place to collect risk information at the activity level, where most operational risks materialize, and to aggregate this information to a level senior management and regulators care about. A best practice approach that's been endorsed by the Institute of Internal Auditors is a three-lines-of-defense structure

First Line of Defense

Operational managers, or process owners, are expected to take ownership and accountability for the risks faced by their business area as a primary line of defense.

Specifically, the IIA recognizes that those working on the front lines of their organization have the task of identifying, assessing, and mitigating risks on a day-to-day basis.

In order to determine if the process owners at your organization are operating as an effective first line of defense, be sure to ask the following questions:

1. Are each of your operational managers assigned a subset of your organization's overall risk library, and can they suggest additions to that subset?

2. Do they have the ability to document control procedures in a way that ties them directly to their subset of risks?

3. Are there adequate supervisory functions in place to notify managers when a control breakdown, or other unexpected event, takes place in upstream or downstream process areas?

Second Line of Defense

The second line of defense is the risk management function, which provides oversight and facilitates the implementation of effective risk management processes.

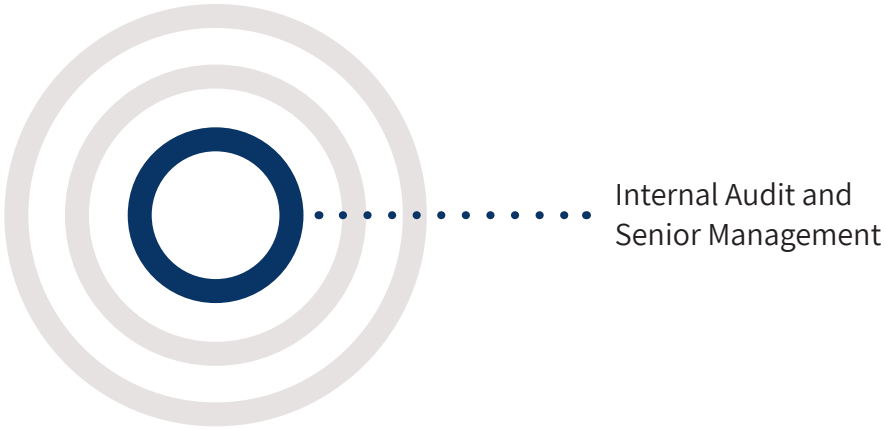
Whereas the first line of defense is process specific, the second line of defense is cross-functional. Risk managers serve the critical role of ensuring that mitigations and risk analyses are taking place as intended, but they cannot independently report on an enterprise picture of risk without input from process owners.

The responsibilities of an enterprise risk manager can include:

- Providing a risk management framework
- Identifying emerging risks and issues
- Setting standards, criteria, and tolerance levels
- Providing consulting and mentoring to process owners

Third Line of Defense

The third line of defense, internal audit and senior management, offers independent assurance that risk management is operating effectively.



These individuals provide oversight, ensure that ERM is functioning with adherence to legal regulations, and provide strategic direction to ensure that risk management activities are aligned with the goals of the organization.

With clearly defined strategic objectives, the risk manager's role is then to close the gap between strategic-level risk and all the operational risks faced at the front line of their organization.

Tone from the Top

Having these lines of defense in place is a fantastic way to get your ERM program up and running because it's a step towards defining how risk management affects everyone's job description. Most front-line employees wouldn't consider themselves any sort of risk manager, when in fact, they're the first line of defense!

Perhaps the most important roles in an organization that need to understand how risk management affects their job function are those at the top level. Setting the right tone for your ERM program starts at the top with your Board of Directors, and other senior executives. Getting support and approval from these groups exudes a positive risk culture, and leads to better engagement in the risk management processes at all levels of the organization. The more integrated ERM is in everyone's job descriptions; the easier risk assessments will become, and the more valuable they will be.

Present ERM to the Board

Download our eBook for actionable tips on presenting the effectiveness of your ERM program and getting buy-in from the Board.

Effective Risk Identification and Prioritization

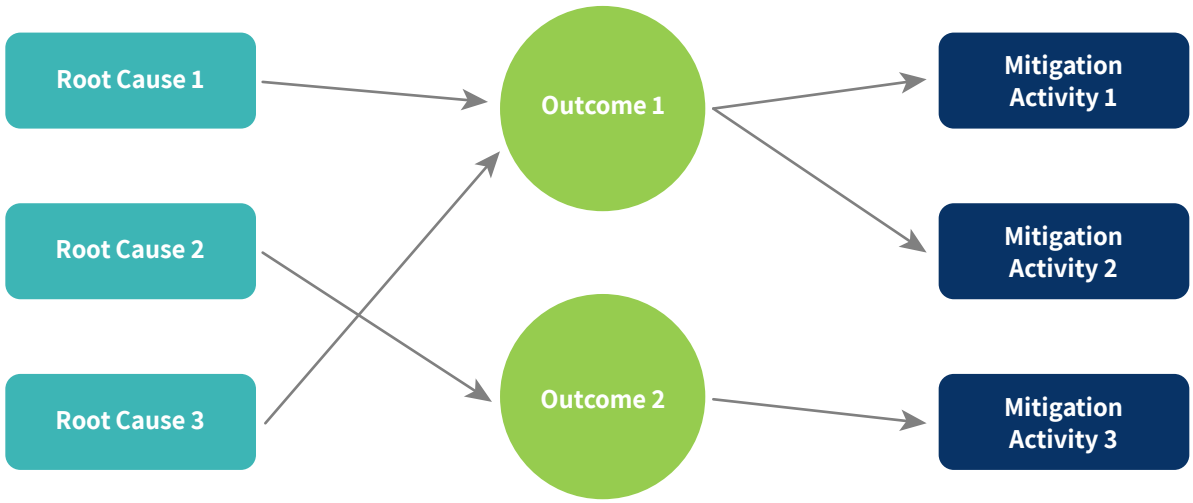
Just discussing high- level concerns with senior executives may have been sufficient 2-5 years ago, but with high expectations from all angles – the board, regulators, external stakeholders – today's risk assessments are required to deliver more business value and better decisions. Formalized risk assessments allow risk managers to leverage existing activities in an objective, quantifiable, and repeatable manner.

Successful companies leverage their risk assessment process to provide strong evidence of how risks and activities at the process level are impacting strategic objectives.

Identifying Root Cause

Companies with successful risk management programs collect data around the root causes of their risks. It is impossible to get a clear picture of strategic objectives without breaking them down into actionable, silo-specific activities. Identifying the root cause of a risk provides information about what triggers a loss, where an organization is vulnerable, and where resolving systemic risks can lead to efficiency gains.

Orientating process owners to root cause is often easier said than done. Typically, senior management tends to think in terms of outcomes, or events they want to avoid or achieve, and the effects of such events. While there are a limitless set of outcomes, as risk managers we need to operate at the root cause level in order to design effective mitigation activities.



Many risk managers find it's hard to engage multiple departments because they're unfamiliar with risk management as a discipline and therefore aren't sure how to communicate it. As you can imagine, talking about the same root causes, outcomes, or mitigations in different ways can cause unnecessary road blocks.

Here's a popular best-practice way to name, categorize, and talk about different kinds of risk.

External

Risk caused by outside people, environment, and other circumstances.

Examples: Fluctuations in economic markets, weather-related hazards or disasters, lack of public infrastructure

People

Risks involving people who work for the organization.

Examples: Misuse of confidential information, willful noncompliance with policies, lack of necessary skill sets

Process

Risk arising from the organization's execution of business operations.

Examples: Inadequate budgeting, missing documentation, lack of policies or procedures

Relationships

Risk caused by the organization's connection with third-parties.

Examples: Contracts are not reviewed properly, inadequate security protocols on third-party relationships

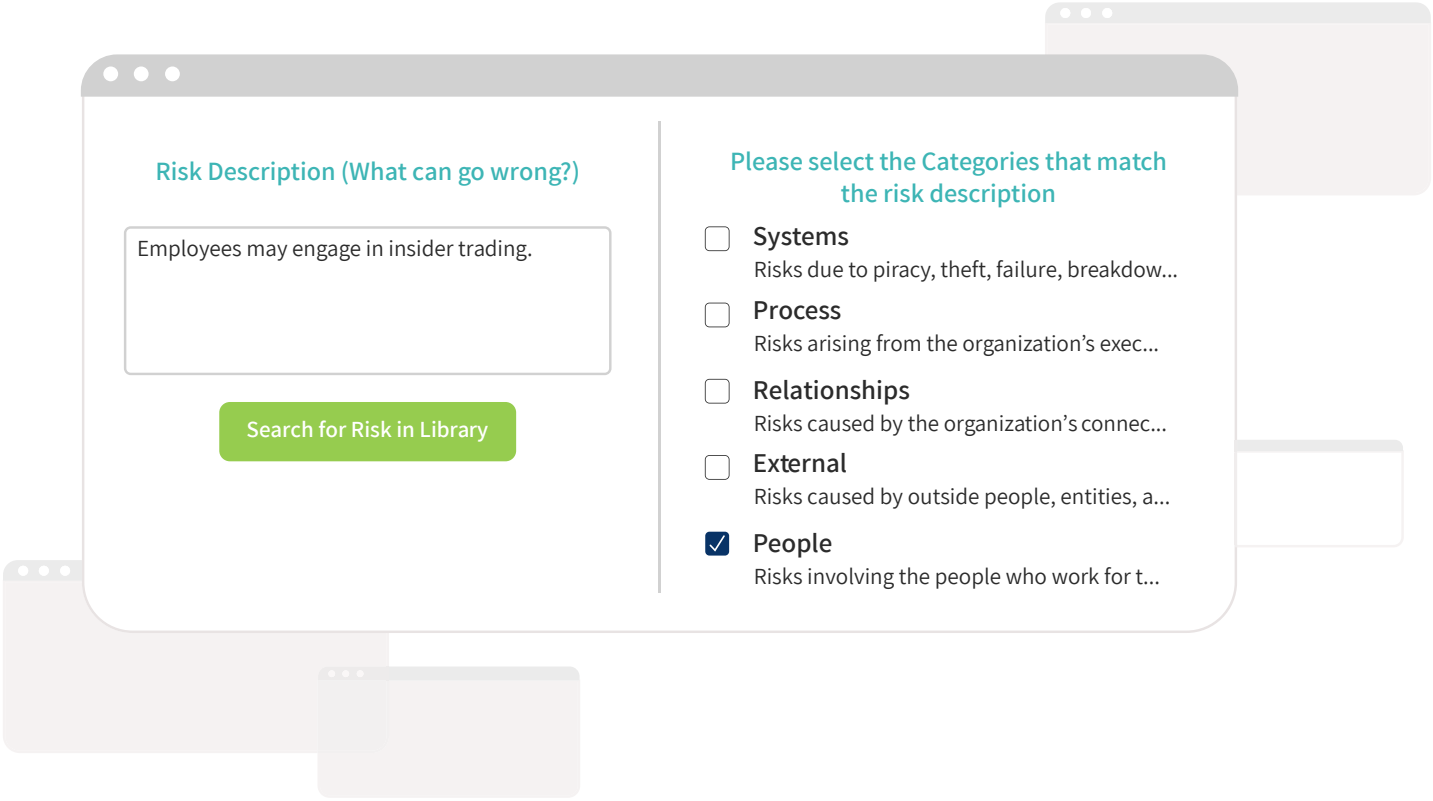
Systems

Risks associated with IT processes, security, data, or information assets

Examples: Data is inaccessible, failure to adopt new technology trends, inadequate system maintenance

Most risk assessments jump right to the “what could go wrong” aspect of risk identification, which is often just a detailed effect or symptom. Understanding the root cause requires identifying the drivers of the risk. You can begin to implement this root cause approach in a facilitated session, or you can use a system to prompt assessors on the root causes of their concerns. These activities will help implement a solution on an enterprise scale.

To start, consider prompting process owners and business areas to select the root cause category of their concern from a pre-built library. Beginning with a root-cause risk library enables organizations to track the selection of root-cause risks across multiple business areas. This helps to identify systemic risks throughout the organization, as well as areas of upstream and downstream dependencies.

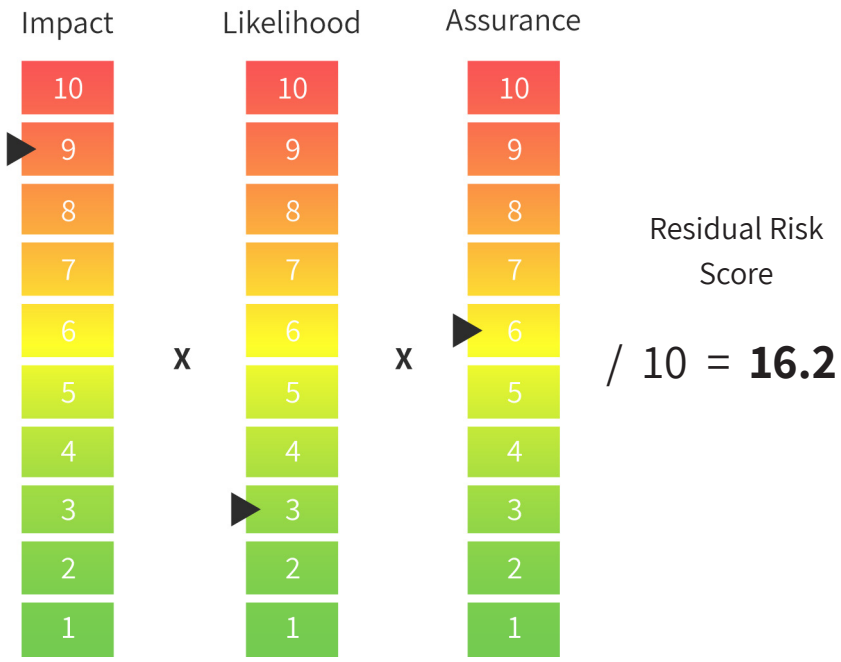


Standardize Numerical Scales

After you've created a system for labeling or identifying risk, you can move on to assessing the potential impact of each risk. A lot of organizations use a high-medium-low scale to assess their risks, but this actually isn't best practice.

High-medium-and low scales make it difficult and time-consuming to quantify, aggregate, and objectively rank information. With only three options from employees to choose from, they'll likely feel conflicted about which to one to choose. Many employees may even feel compelled to write in a medium/high option.

In reality, best practice favors a 1-10 scale, with 10 having the most unfavorable consequences to the organization.



Using a 1-10 scale makes calculating the residual index score of a risk more straight forward. Giving employees more flexibility in their assessments will increase accuracy, and more confidence when determining what your top risks really are.

Standardize Evaluation Criteria

Having more numerical options for employees to choose from when assessing risk is a good start, but in actuality, even a 1-10 scale can present opportunities for miscommunication. For example, someone's 7 could be another person's 9. This is why it's equally important to standardize your evaluation criteria, or in other words, provide guidelines for what makes a 7 a 7, as opposed to a 9.

There are multiple ways of expressing severity, both qualitatively and quantitatively. Severity should be outlined in terms of financial, legal, operational, regulatory, and strategic dimensions. Each of the 5 buckets should have a variation of criteria applicable to that level of severity.

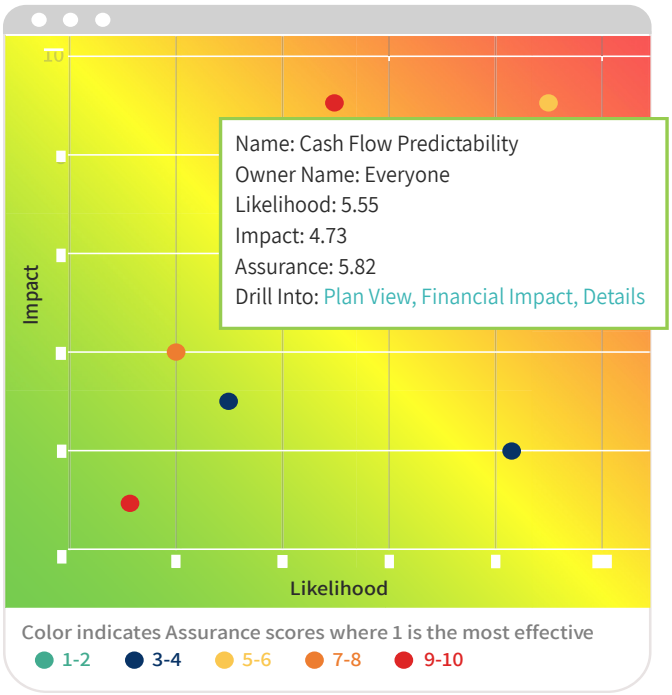
1 – 2 Insignificant	3 – 4 Minor	5 – 6 Moderate	7 – 8 Serious	9 – 10 Major
• **Financial** • **Legal** • **Operational** • **Regulatory** • **Strategic**	• **Financial** • **Legal** • **Operational** • **Regulatory** • **Strategic**	• **Financial** • **Legal** • **Operational** • **Regulatory** • **Strategic**	• **Financial** • **Legal** • **Operational** • **Regulatory** • **Strategic**	• **Financial** • **Legal** • **Operational** • **Regulatory** • **Strategic**

You can then set a guideline for each severity category as it pertains to each risk score.

7 - 8 Serious	9 - 10 Major
• **Financial**: Negative impact on net income – $15 million to $20 million • **Financial**: Alternative financing (debt), sale or restructuring of the organization could be required • **Operational**: Inability to remain competitive (e.g., lagging customer service, operational inefficiencies) • **Regulatory**: Regulatory penalties are required	• **Financial**: Negative impact on net income – over $20 million • **Financial**: Catastrophic impact on financial statements (e.g., critical contractual ratios are no longer met) • **Operational**: Long-term impairment of critical functions make the organization vulnerable to forced sale of merger • **Regulatory**: Regulatory agencies seize control of assets or are granted absolute decision-making authority

Only one of the criteria listed for an impact level has to be met in order to rate a risk factor at that level. This way, any qualitative criterion can be given a score to become quantitative and comparable across the enterprise.

Now that your assessment scores are numerical and comparable, you can create simple formulas to automatically calculate the inherent and residual indexes of risks This allows for risks across your organization to be sorted and objectively ranked.



Process/Other Dimension		Residual Index
Strategic Imperatives		
Cash Flow Predictability	C	18.15
Reputation	E	8.93
Corporate Branding	A	27.37
Talent Management	G	5.66
Employee Safety	H5	.41
Operating Expenses	B	19.62
Sustainability	D	14.08
Cybersecurity	F	8.73

For Board reports, you could aggregate risks relating to the same strategic goal or other cross-functional topics, like risk category frameworks and regulatory standards. This provides an overall assessment score for leadership, with actionable underlying data for when direction is given.

Improve Your Risk Assessments

Download our eBook, "5 Steps for Better Risk Assessments," for more information on how to standardize and leverage your risk assessments.

Actionable Risk Appetite Statements

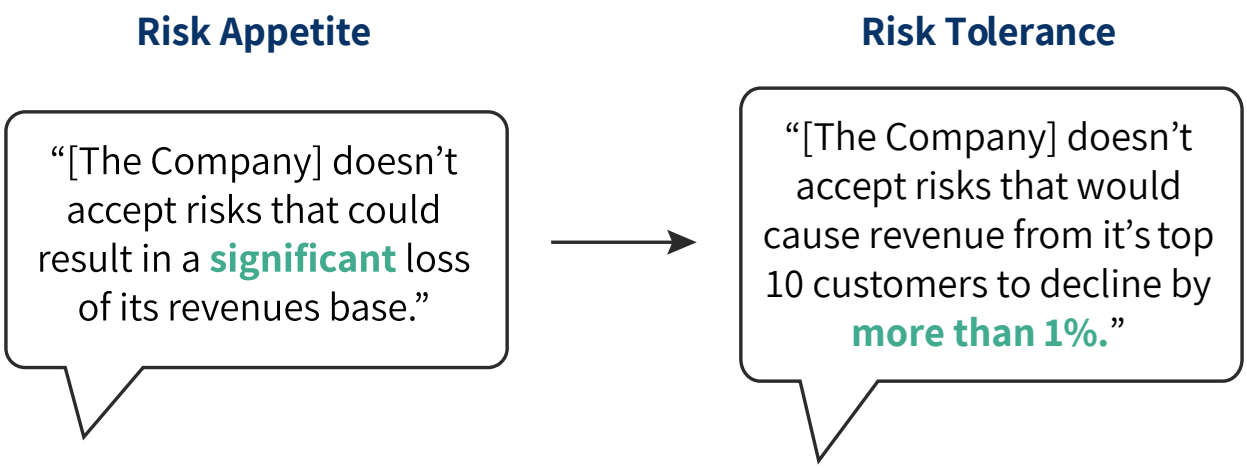
According to ISO 31000, risk appetite is, “The amount and type of risk that an organization is prepared to pursue, retain or take.” An organization-wide risk appetite can be a powerful tool that gives your risk program direction. However, like any policy, without an accompanying action risk appetite is nothing more than an idea.

So how do you make risk appetite actionable? Implement risk tolerances.

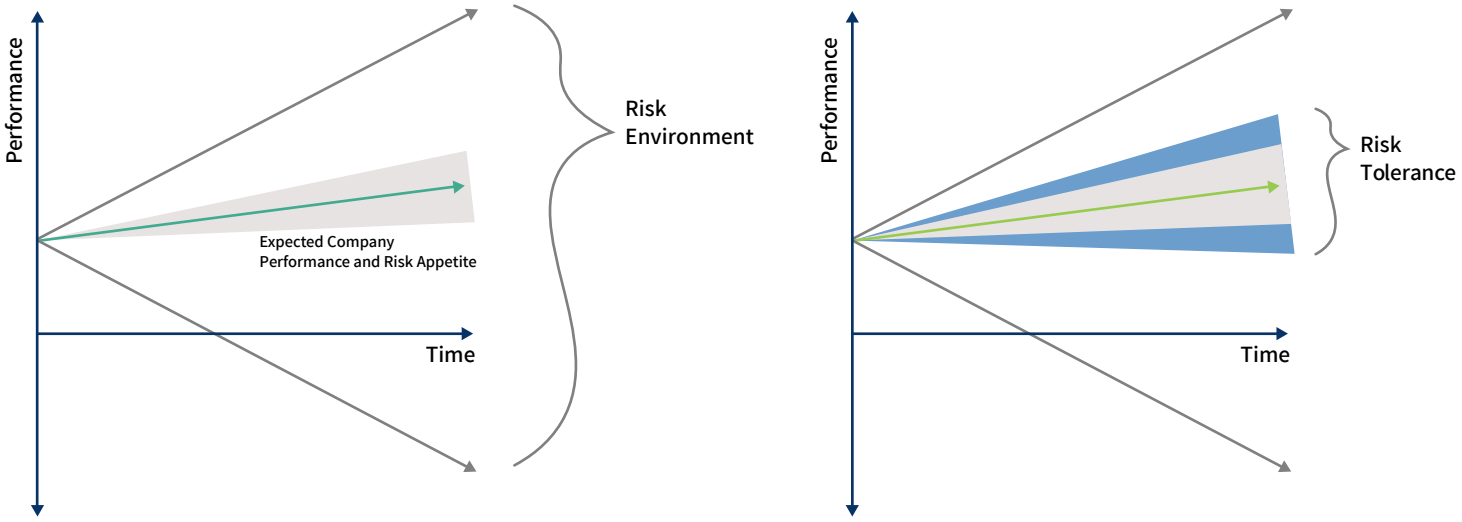
Risk Appetite vs. Risk Tolerance

Risk appetite and risk tolerance both set boundaries on how much risk an organization is prepared to accept. 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 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 risk tolerance.

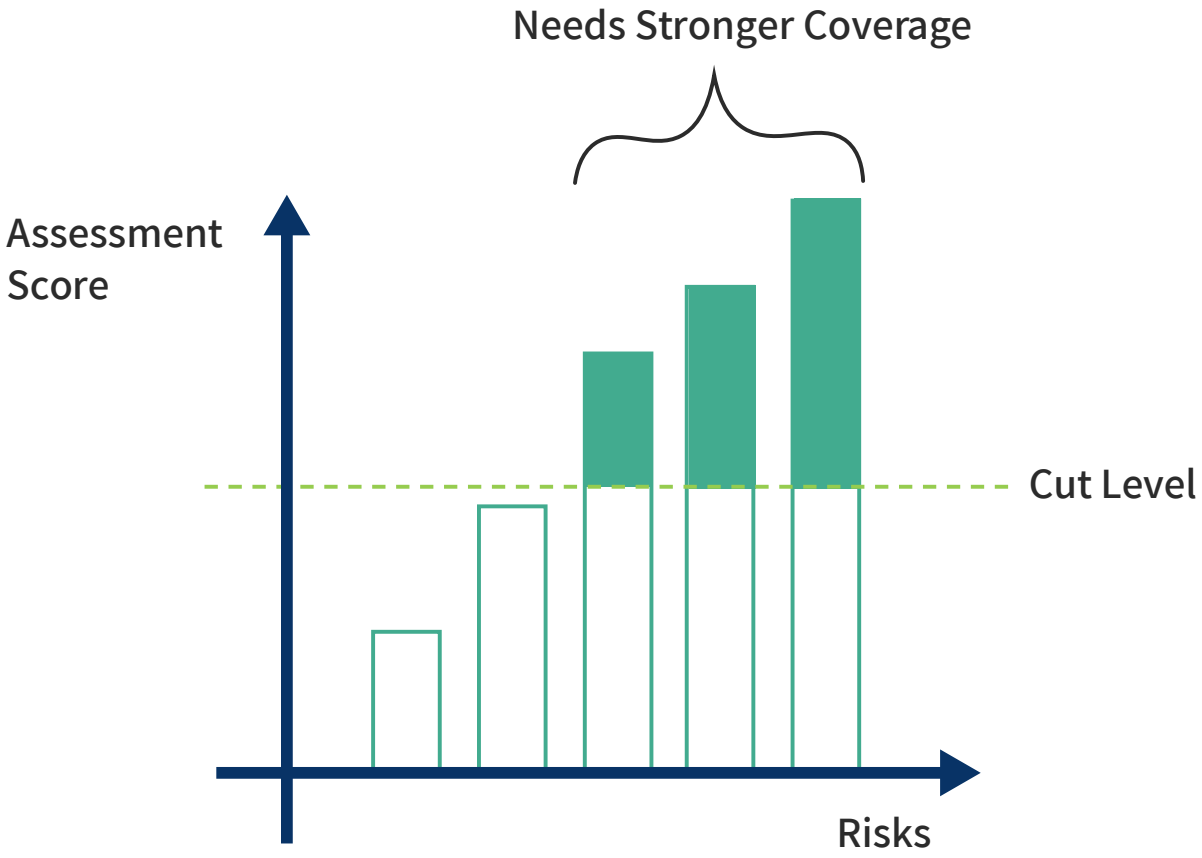


Let's look at a graphic representation of risk appetite and risk tolerance. In the charts below, the organization's projected path of performance is plotted in green. This line and the immediate area around it represents the risk appetite, or goal of the organization. If the organization was to pursue 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.

Take Action on Your Risk Appetites

If you're looking for more ways to make your risk appetites more actionable, download our free copy of our eBook, "5 Steps Towards an Actionable Risk Appetite."

Centralized Risk Monitoring Activities

Once you have identified the root causes of your risks, and have objectively assessed them, you need transparency into “if” and “how” risks are actually being covered by controls. Oftentimes, the knowledge of “how” a risk is mitigated is a conversational explanation from the business area. But, this is only sufficient for some risks.

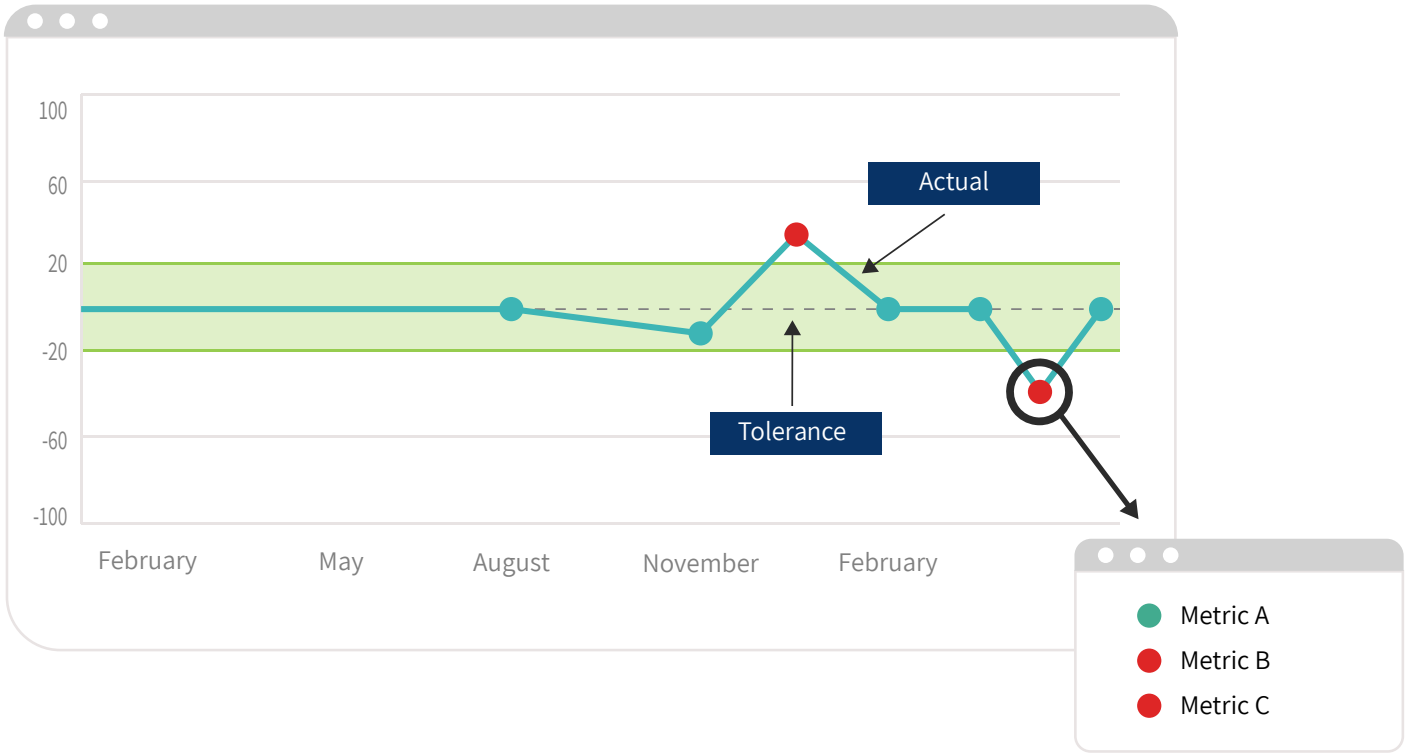
This is why successful companies believe it’s critical to ensure that all of their mitigation activities are adequate in addressing their top risks.

Risk managers need to be responsible for risk monitoring effectiveness. This means that risk managers need to know what to monitor, and how to determine if their activities are effective. To begin, follow these three steps:

1. Allow risk tolerances to develop over time
2. Eliminate areas of upstream and downstream dependencies
3. Prioritize activities and initiatives to be monitored
4. Collect and monitor business metrics

Allow Risk Tolerance to Develop Over Time

As risks are re-assessed periodically, you'll learn to focus on emerging risks as they become out of tolerance and spend less time on risks that have decreasing indexes. This allows you to allocate your resources to the issues and areas that will yield the greatest benefits to the organization.

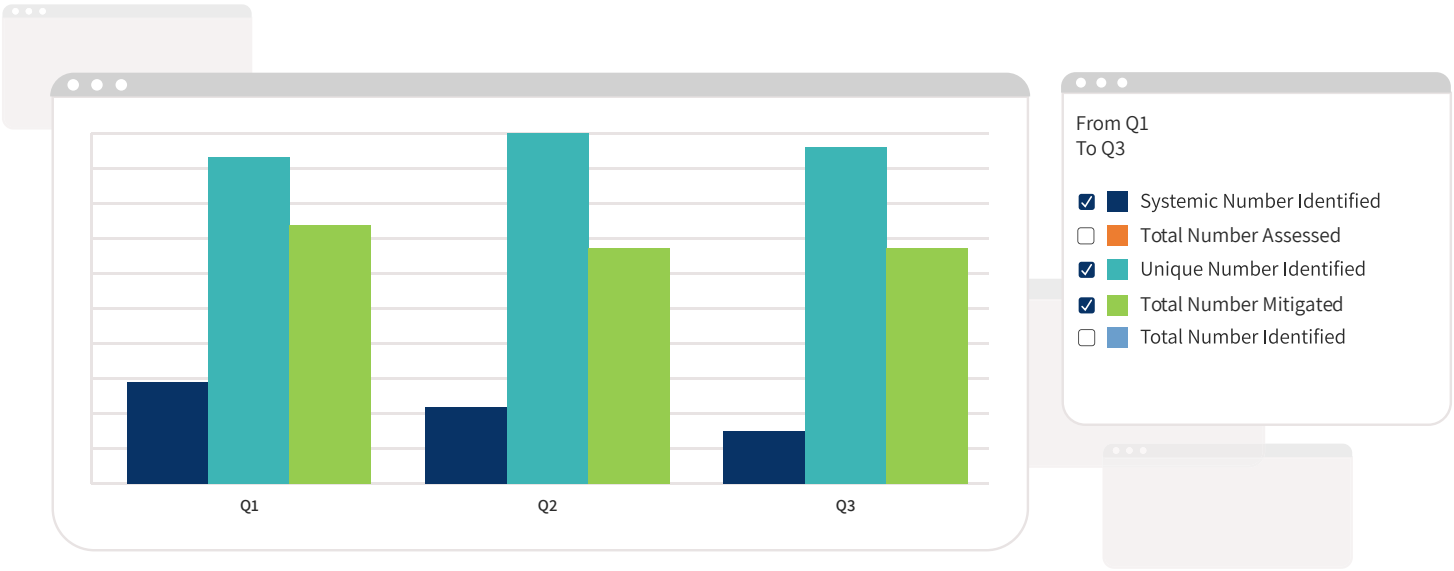


Eliminate Areas of Upstream and Downstream Dependency

A lot of organizations manage their company's risks in silos, meaning IT risk is handled within the IT department, financial risk is handled within the finance department, and so on and so forth. The problem with this approach is it facilitates too many opportunities for oversight. Plenty of risk exists in between silos, such as in the relationship between finance and IT. A silo'd approach also means work is being duplicated where it doesn't have to be, as oftentimes multiple departments are collecting and analyzing the same pieces of information.

The hallmark of an effective ERM program is taking an integrated approach to risk management by centralizing the information collected and designing a system to identify relationships between risks, departments, personnel, initiatives, and other facets of a business. We call this system a **risk taxonomy**.

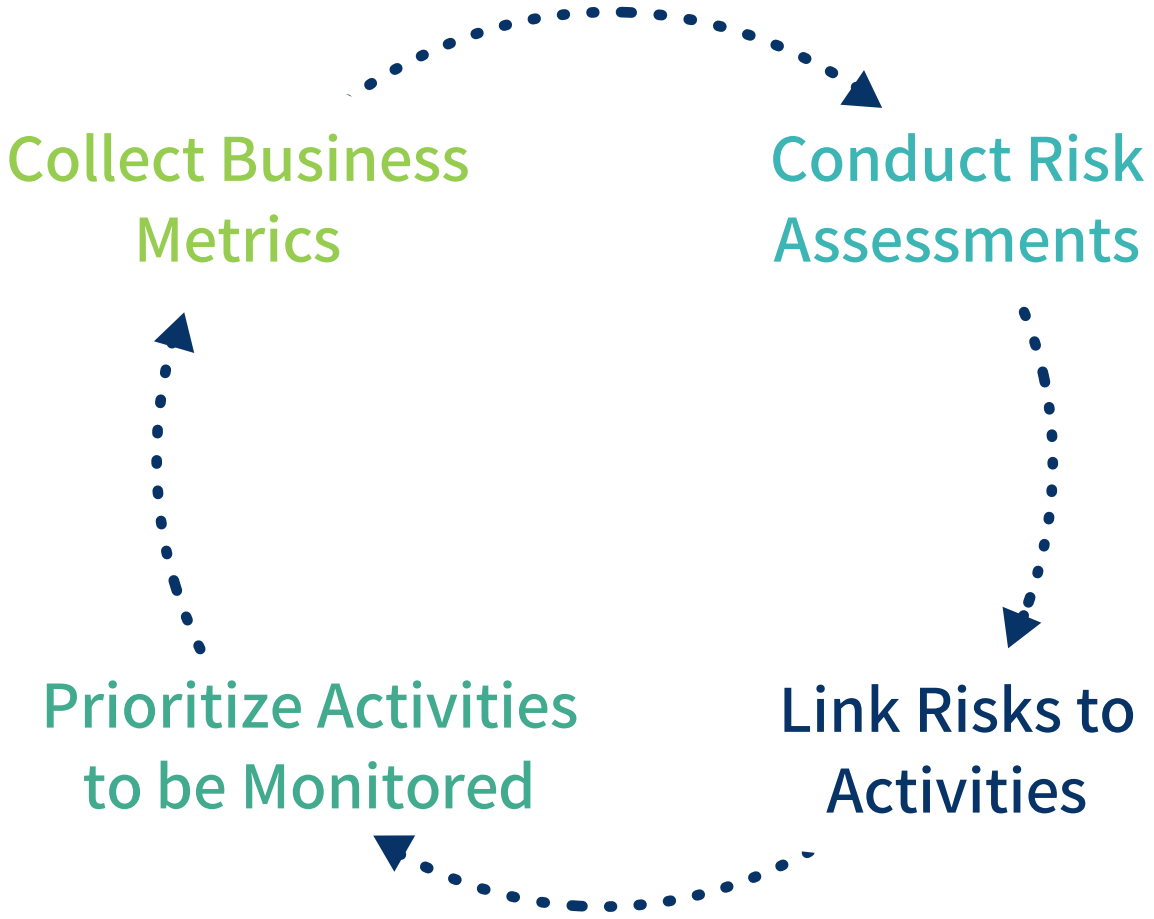
Systemic risk identification will detect areas of upstream and downstream dependencies throughout your organization such as when one area of the organization is unknowingly causing strain on other areas. This method also identifies areas that would benefit from centralized controls.



Prioritize Activities and Initiatives to be Monitored

As we said in the previous section, a risk taxonomy will allow you to create relationships between all kinds of facets of your business. A simple, yet often overlooked, relationship you should create is the one between risks and their control activities. Every company has mitigation activities in place, but the question arises, how many people really know which activities are designed to keep which risk in tolerance?

There are many benefits to linking control activities to the risks they're meant to address. First, creating these relationships allow companies to begin the process of prioritizing which activities need to be monitored. Second, when a risk or activity changes, you'll have a better understanding of how these changes will affect the metrics you're collecting.



Collect and Monitor Business Metrics

For this step, let's look at a brief example of the different ways organizations can collect metrics on a control they've implemented.

Problem	An online banking system consistently experiences significant downtime, and the issue is not resolved in a timely manner.
Root Cause	The personnel who have the necessary expertise to fix the problem are usually not available during down time.
Control	Cross-train more individuals with the necessary technical skills.

Now, how can you measure whether this control is actually solving the problem?

Testing will only get you so far.

Often, organizations get caught up in testing the compliance or occurrence of the control, such as: "Has every new IT hire completed the cross-functional training program within their first 6 months of employment?" This pass or fail test provides a high-level view of whether a control is occurring. Unfortunately, this kind of testing does not provide you with actionable steps that will help you improve a mitigation activity.

Collecting business metrics provides actionable insight.

Collecting business metrics enables you to track the progress of your mitigation activities over time and understand the "why" behind the mitigation activities that are currently in effect. In this situation, if the bank collected specific metrics about the system downtime and monitored them over time, they would have seen that there was no improvement from the control put in place. This would have caused them to investigate further and see that the system was going down during peak usage times, like lunch, when the subject matter experts were away from their desk! They could then institute more effective mitigation activities, like adding more memory to the system.

What other metrics can you collect?

Download our eBook, "Meaningful Metrics: Using ERM to Inform Strategy," to see some actionable risk metrics that can improve efficiencies, identify new opportunities, and prevent risk events.

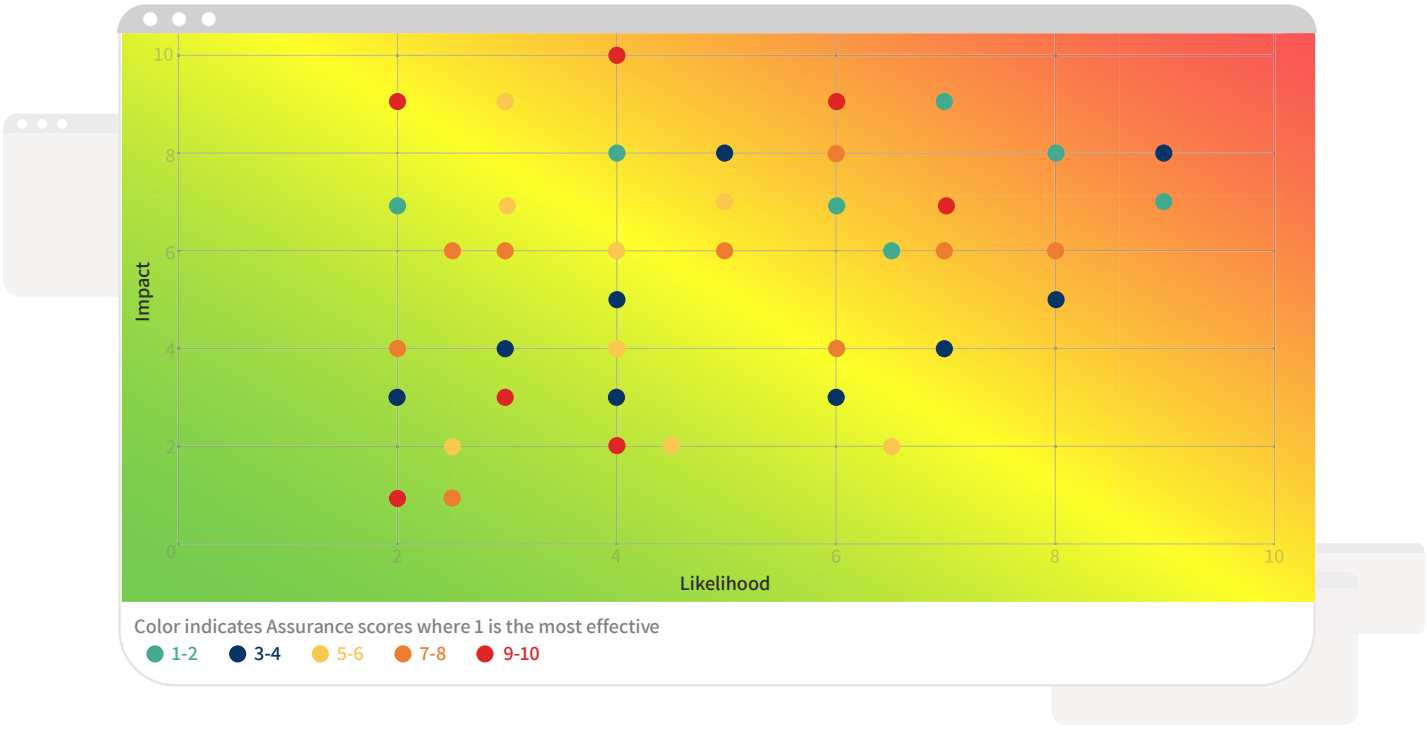
Forward-Looking Risk Reporting

Once you've standardized your risk assessments and have implemented effective mitigation and monitoring activities, you'll find yourself with a lot of detailed risk information. The question then becomes, how do you report all of this information and communicate the results in a way that demonstrates the value of your ERM program?

Compiling best-practice risk reports and presentations for senior executives at any company is not an easy task. Risk managers must first be able to demonstrate how risks across the organization will roll up to impact the Board's strategic objectives and key concerns. Secondly, they are expected to provide key metrics that validate the effectiveness of the risk management approach the organization is taking.

In this chapter, we'll cover three views of risk that you'll want to present to your company's leadership team on an ongoing basis.

The Risk Heat Map: Display Your Organization's Most Critical Risks



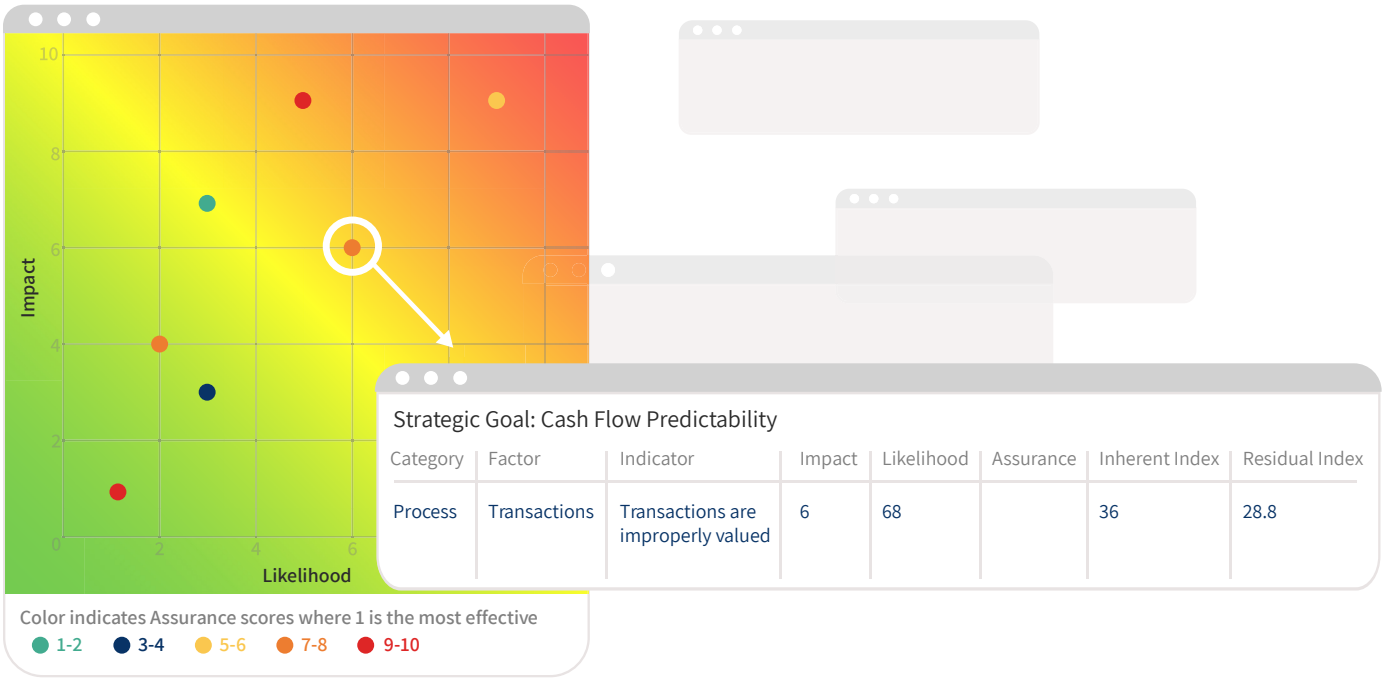
One of the main benefits of adopting a common set of standards and assumptions for your risk assessments is that all of your organization's risks can be brought together and displayed on a heat map. This way, you're comparing apples to apples and not oranges.

Now you can be sure that the risks displayed in the upper right-hand corner of your company's risk heat map are the most critical risks across business groups.

This high-level heat map displays all of an organization's risks, across functions and levels. You'll want to update your heat maps regularly, so that the information stays current and changes in assessments are reflected.

The Enterprise View: View Risk By Strategic Goals

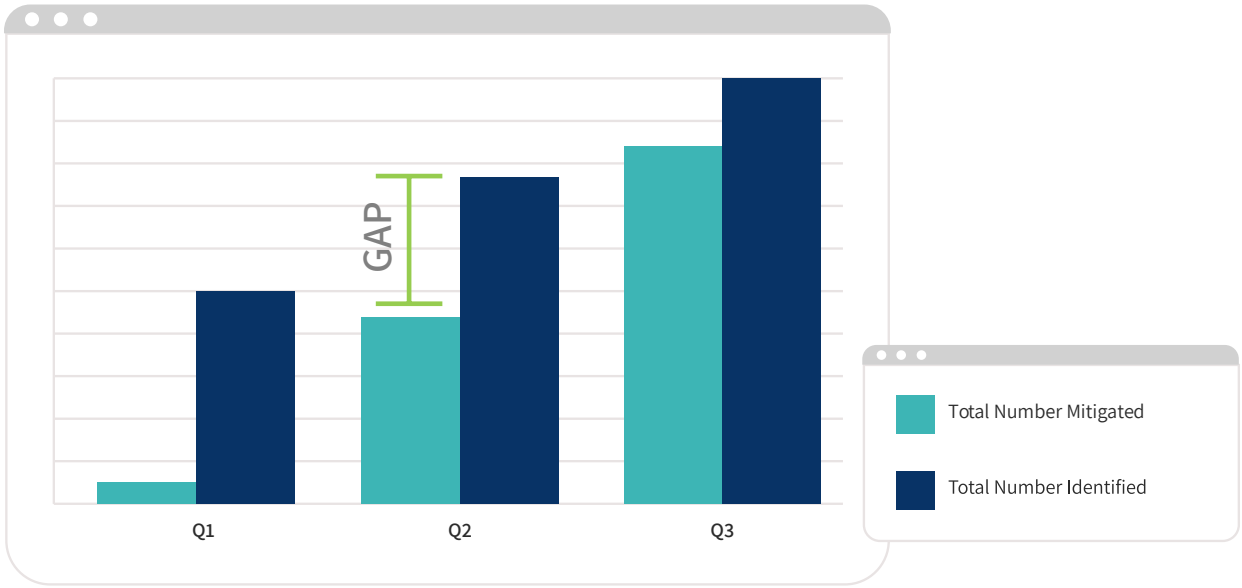
Often, risk managers need to provide more detailed underlying data for risks that affect strategic goals such as which business areas are involved, their individual risk profile, and what mitigation and monitoring strategies are in place. By leveraging your risk taxonomy, you can easily pull up that information and create a more granular dashboard for objectives like "cash flow predictability."



The Progress of Your Program: Risks Identified and Mitigated

Risk management is a process, and the key to successfully monitoring the effectiveness of any process is measurement. A simple yet effective way to present the success of your ERM program is to show the difference between risks you've identified and risks you've designed mitigation activities for.

Over time, you'll be able to show the gap between these two metrics getting smaller and smaller.



As we discussed earlier, all assessments should be standardized with a common numerical scale and criteria throughout your organization so you can give each risk a residual risk index score. This allows you to filter this gap by using a cut level, focusing only on risks above a certain tolerance threshold. For example, you could limit your display to only risks that are rated at "above average" levels.

You could also leverage your taxonomy to filter this view by risks identified and mitigated within a certain department or those that affect particular strategic goals. It's important to make your reports as flexible as possible so they can present what's most interesting to a diverse set of audiences.

Build an ERM Program with LogicManager

There's a lot going on in this eBook. But have no fear! The most successful companies with the best ERM programs take it one step at a time. Take some time to think about which of these characteristics would benefit your company the most, and remember that they build off of each other, so once you've gotten yourself one win, you're well on your way to the next.

Many companies, however, find it easier to implement these five characteristics with the help of ERM software. Request a demonstration to see how LogicManager can help you communicate across departments, collect actionable information, and report on your success.

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

+1 617 530 1210 | logicmanager.com | info@logicmanager.com