LOGICGATE

KRIs for ERM:
Developing Metrics for Managing Enterprise Risk

Table of Contents

01 Introduction

02 What is a key risk indicator (KRI)?

03 How are key risk indicators used in enterprise risk management?

06 KRIs vs. KPIs: Similarities, differences, and interconnectedness

07 How to develop KRIs

16 KRIs in the Wild

20 Conclusion

Introduction

Stop us if you've heard this one before: "You can't manage what you don't measure." This phrase has become one of the most popular adages in business, and it cuts to the core of one of the most important movements of the past few decades: becoming data-driven.

The era of digital transformation has flooded organizations of every shape and size with data, drawn from a galaxy of digital systems and platforms, data brokers, public databases, and other sources. In 2023, the world is expected to produce and consume 118 zettabytes of data — and that's only expected to increase as we digitize...well, just about everything.

Every business function—from engineering to marketing to research and development— harnesses this new and suddenly plentiful resource in different ways to drive positive outcomes, and risk management is no exception. There's more information readily available about every threat on our risk landscape than ever before, and that provides risk leaders an opportunity to leverage insights drawn from data to predict or anticipate when threats may strike.

At the same time, the global regulatory landscape is growing more and more complex, and risk management is being more closely scrutinized by auditors, executive teams, and boards of directors than ever before. All are demanding timely, relevant information on how organizational risk is being handled.

That's why, here at LogicGate, we've adapted that famous business mantra a bit and added our own risk management twist: "**The better you measure risk, the more effectively you can mitigate risk.**" And, measuring risk properly makes it easier to turn it into a strategic advantage.

In practice, the best way to do this is through developing effective key risk indicators, or KRIs. These metrics take all that data and distill it into proactive insights for managing risk.

Having a good set of clear, measurable KRIs:

- Reduces uncertainty
- Increases operational resiliency
- Improves risk program efficiency and resource allocation
- Helps uncover concerning trends before they become a problem
- Uncovers strategic opportunities
- Informs decision making
- Empowers ERM leaders to move from reactive to proactive, holistic risk management

This guide is designed to help you start building key risk indicators and put them to good use at your organization, from the most basic dashboard all the way up to advanced monitoring and automation techniques. Let's dive into the world of KRIs and data-driven enterprise risk management.

What is a key risk indicator (KRI)?

Key risk indicators are metrics designed to provide early warning of potential risk events. Typically, KRIs take their input from external or internal data sources and estimate the overall likelihood that the risk being monitored will occur, how fast that could happen, and how much damage it will cause to your organization if it does. Each is ideally tied to the thresholds in your risk appetite, and if the metric exceeds a particular threshold, action plans are triggered.

In short, KRIs are basically tripwires for detecting risk before it causes problems for your organization.

Think of it this way

You could live in a house without fire alarms and make sure to have a fire extinguisher on hand in the event that a fire breaks out, but that's a pretty risky and flat-out dangerous way to approach things. Your first clue that there's trouble could be flames or smoke in your bedroom, and by then it might be too late. That's why we install fire alarms and regularly check their batteries: The alarm, constantly monitoring for the presence of smoke, is your KRI, and the shrill siren going off notifies you that your threshold—the moment something catches fire—has been exceeded. That can allow you to act faster to douse the flames, escape the building, or notify the fire department.

Or, let's raise the stakes a bit

Militaries around the world invest significant sums of money in making sure it's able to detect missile launches, signals intelligence, cyber attacks, troop movements, and other signs of aggression from foreign powers, terrorist groups, or other non-governmental actors as early as possible. The data each of those systems provides can be considered key risk indicators for national defense.

We saw this in action when the United States military was able to make evidence of Russia's military build-up along its border with Ukraine public ahead of the February 2022 invasion. Russian military activity was the key risk indicator, and the observed deployments exceeded the threshold for action—which took the form of diplomatic efforts to head off a conflict, the bolstering of Ukrainian defenses, and strategic coordination among the members of NATO.

Not every organizational risk is going to have the extreme impact of an international military conflict or structure fire, but having the right KRIs in place can provide advance warning about whatever risks you want to avoid.

How are key risk indicators used in enterprise risk management?

Let’s shift back over to the business world and explore how KRIs can be used to effectively manage enterprise risk.

1 Moving from a reactive to a proactive stance

The most obvious benefit of having a good system for tracking KRIs is that it allows you to anticipate and formulate responses to risk events, rather than simply waiting for them to materialize and deciding how to respond on the fly.

The foresight provided by KRIs is the foundation of a proactive risk management program, and the more proactive your program is, the stronger your overall organizational security will be.

Take the risk of a global recession, for instance. As inflation began ticking higher and higher in 2021, many businesses viewed the rising rates as a key risk indicator that the Federal Reserve and other central banks may begin raising interest rates to reverse the trend.

Since that sort of activity often precedes an economic downturn, both rising inflation and expected interest rate hikes can be used as KRIs to warn businesses that it might be time to start cutting costs proactively and shoring up reserves in anticipation of tougher times ahead, rather than waiting until conditions had already deteriorated.

2 Streamlining audits and reassuring clients

KRIs are also useful in ensuring that your organization is in compliance with any regulations you're required to operate under, like HIPAA or SOX, or whichever security frameworks you choose to implement, like ISO 27001, NIST, or SOC 2. Showing up armed with data and evidence when audit time rolls around can streamline the process, reducing the likelihood of negative findings.

Being able to prove to clients that you're on top of organizational risk and cybersecurity can also provide reassurance and improve your relationship with them. That can turn into a competitive advantage if your competitors can't prove the same diligence.

3 Improving risk prioritization

KRIs take the guesswork out of prioritizing risks and making decisions around where to focus your risk management efforts. When combined with risk quantification methods that attach financial impact projections to your risks, like Monte Carlo simulations and the Open FAIR™ model, KRIs allow you to move beyond more subjective methods like ordinal charts and make better, faster risk decisions.

4 Getting buy-in for risk management initiatives

It's extremely difficult to get buy-in for implementing your risk programs from leadership or the board if you can't explain why it should be a priority in the clearest possible terms. Presenting them with a chart or visualization showing where your threshold for a certain risk is and how the KRIs that would trigger action are trending—especially if you can tie financial impact figures to the risk in question—is one of the most effective ways to do this.

5 Identifying strategic opportunities

On the flip side, KRIs can also help leadership understand where mitigating, avoiding, or even embracing a particular risk could lead to a strategic advantage. The more robust your system for tracking KRIs is, the more likely you'll be able to stay on top of and seize on these trends, while your competitors may not notice them at all.

KRIs vs. KPIs: Similarities, differences, and interconnectedness

While KRIs are similar in many ways to their close cousin, the key performance indicator (KPI), there is at least one fundamental and significant difference.

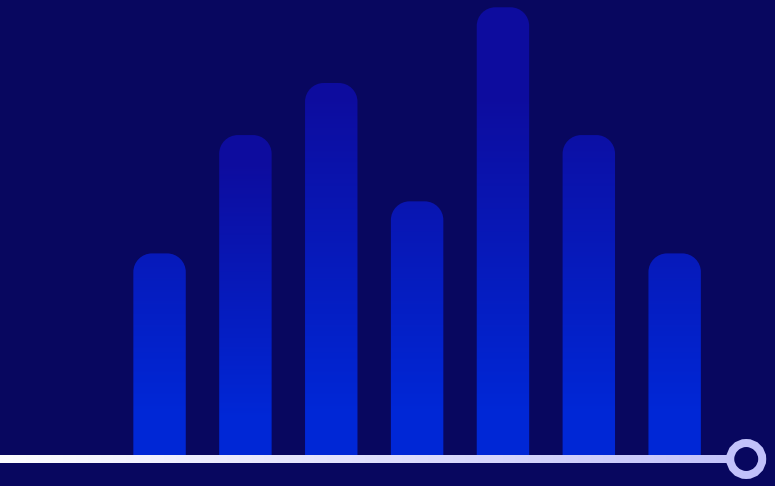
KPIs are most commonly designed and used to measure past performance, such as progress towards revenue goals, return on investment in a new tool or system, or adoption of a new product or service.

KRIs, on the other hand, are more proactive in nature. They're meant to keep an eye on trends that could lead to problems for your business, so you can get ahead of them and make strategic decisions that will allow you to avoid the worst outcomes.

But under certain circumstances, KRIs can also act as KPIs. Say your organization has had problems with phishing, and your cybersecurity team recently deployed new technology for running simulations to help employees avoid becoming the victim of phishing. Setting KRIs to track the number of real phishing attacks directed at your organization, the number of successful phishing attacks, the number of employee-reported suspicious emails, and the number of failed simulated phishing attacks can help you validate whether your efforts to prevent such attacks are paying off or if they need to be reworked.

How to develop KRIs

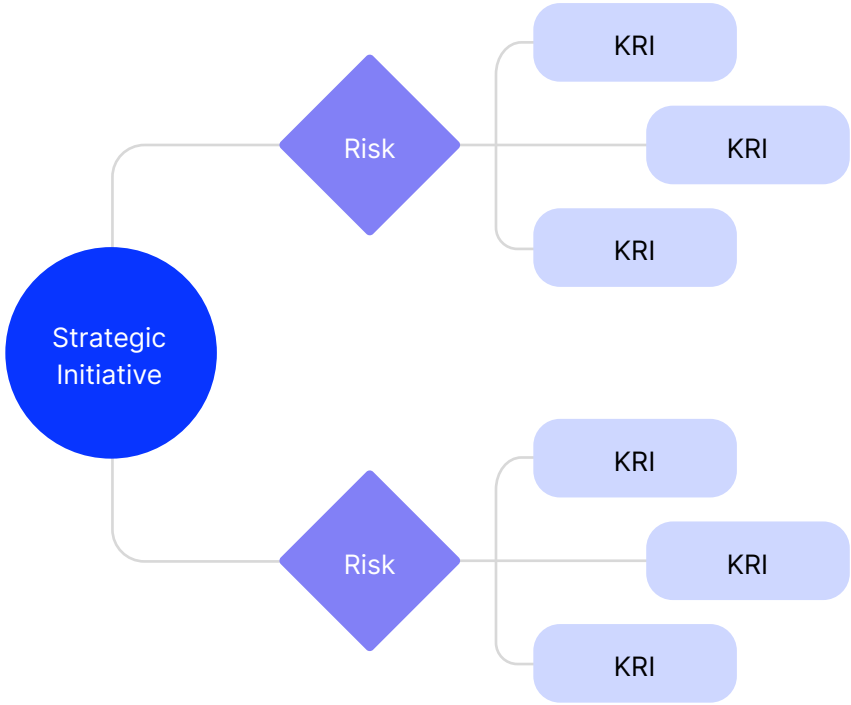
So we've established how useful key risk indicators can be. Now we'll dive into the best way to start building them for your organization.



Know your business and its strategic priorities

The core reason we practice enterprise risk management is to ensure that the risks and threats facing our organizations are not able to interfere with—or even completely derail—our strategic objectives and initiatives. So, the first step in developing KRIs should be to take stock of all of your risks and map each one to the strategic initiatives they have the potential to impact.

Mapping Risks To Inits



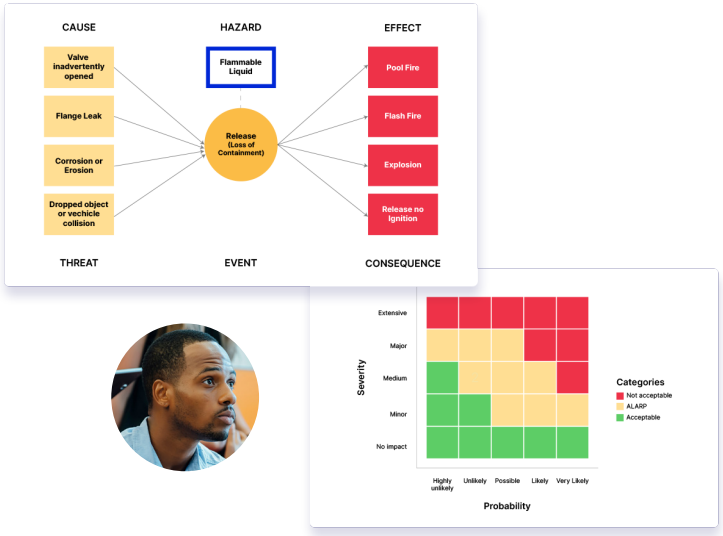
Rank your risks

Once you have your risks bucketed out and assigned to your objectives, it's time to stack them up against each other and decide which are the most pressing and should be tracked first. You can use both qualitative and quantitative methods to do this.

Qualitative risk analysis involves conducting research with both your organization's leadership and ground teams, either through surveys or interviews, then drawing insights from the data to rank your risks, typically through the use of ordinal scales, risk matrices, heatmaps, and bow-tie analysis.

Quantitative risk analysis involves using more advanced techniques to estimate the actual monetary loss that your business could experience if the risk in question occurs. Having that level of detail makes it much easier to truly understand which risks pose the greatest threat to your business and obtain buy-in for your efforts to ward them off.

Risk Matrix and Bowtie Analysis



LogicGate's Risk Cloud Quantify

Identify root causes of risk events

Now that you have a clear understanding of which risks you should focus on first, you'll need to identify the right data sources for fueling your KRIs.

You can do this by reverse engineering each risk. In as much detail as you can, think through the sequence of the events that would need to happen for the risk event to occur, then identify each point where a record of each event may exist. Those records can provide the data you need.

In the above example of the company with the phishing problem, the risk is a successful phishing attack that results in a data breach, fines, and significant reputational damage. The root cause can be a lack of security awareness or ineffective controls. So, they'd want to start testing employees with simulated phishing attacks and track how many pass or fail. The number of failed tests and reported emails over the total simulations would be the KRIs in this case.

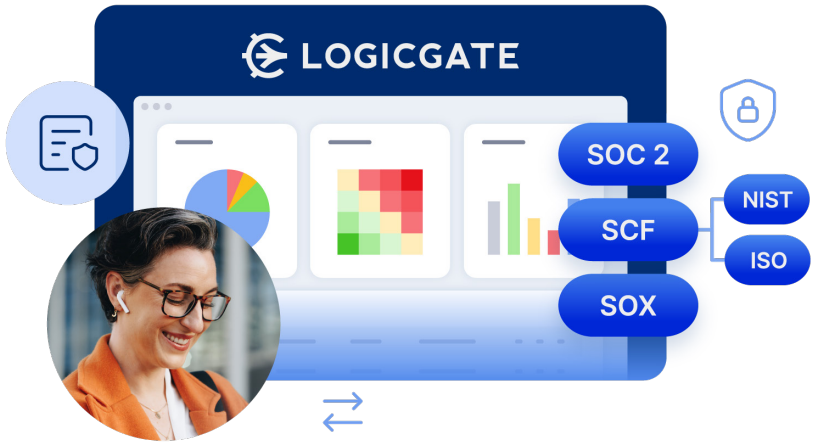
Another root cause could be an overall increase in the number and sophistication of real phishing attacks targeting your company or industry. When the volume of attempts reaches a level that makes the security team uncomfortable or if they'll be making a big announcement soon that could make them a target, the company can begin ramping up cybersecurity training efforts even further.

Ideally, you'd want to set KRIs to track every event from the root cause all the way up to the moment the risk event occurs. This will make sure you have plenty of lead time to respond if the alarm bells start going off.

Centralize your data

Once you've begun collecting the right data, you need a way to centralize, organize, and visualize it all.

This can be done in a variety of ways, but having modern, integrated GRC software is usually the right call. These tools are purpose-built for taking in risk data, either through direct entry by risk owners or automatically through integrations with other business systems, and reporting it in dashboards, charts, and other visualizations. Being able to get a quick look at your risk data in this way will make both monitoring your KRIs for signs of trouble and reporting them to leadership much easier down the road.



Identify, define, and build your KRIs

For your KRIs to be useful, they need to be easily understood by the people who will be using them and relevant to the risks they're monitoring.

1. **Measurable**
   You need to be able to continuously measure your KRI over time to pick up on trends that indicate increased exposure. No available data, no KRI.

2. **Relevant and specific**
   Your KRI should be tied to a particular risk and use data sources relevant to that risk.

3. **Predictive**
   The whole point here is to get ahead of risk, so your KRIs should ideally be leading indicators that catch things before they occur, not lagging indicators that report what happened afterwards.

4. **Benchmarkable**
   It's difficult to set an accurate threshold for taking action if you don't have any information on what normal looks like for your KRI. Make sure you have a benchmark to compare your metric against.

5. **Accessible**
   For a KRI to make a difference, it needs to be clearly defined. The people who will use your KRI to make important decisions should be able to understand it at a glance.

6. **Efficient**
   Developing and maintaining your KRI shouldn't be an unnecessarily time, effort, or resource-intensive task. If you're going to put significant effort into developing a single metric, make sure it's associated with your most pressing risks.

Making sure your KRIs check each of these boxes will maximize their usefulness and optimize the return on the investment you put into building and deploying them.

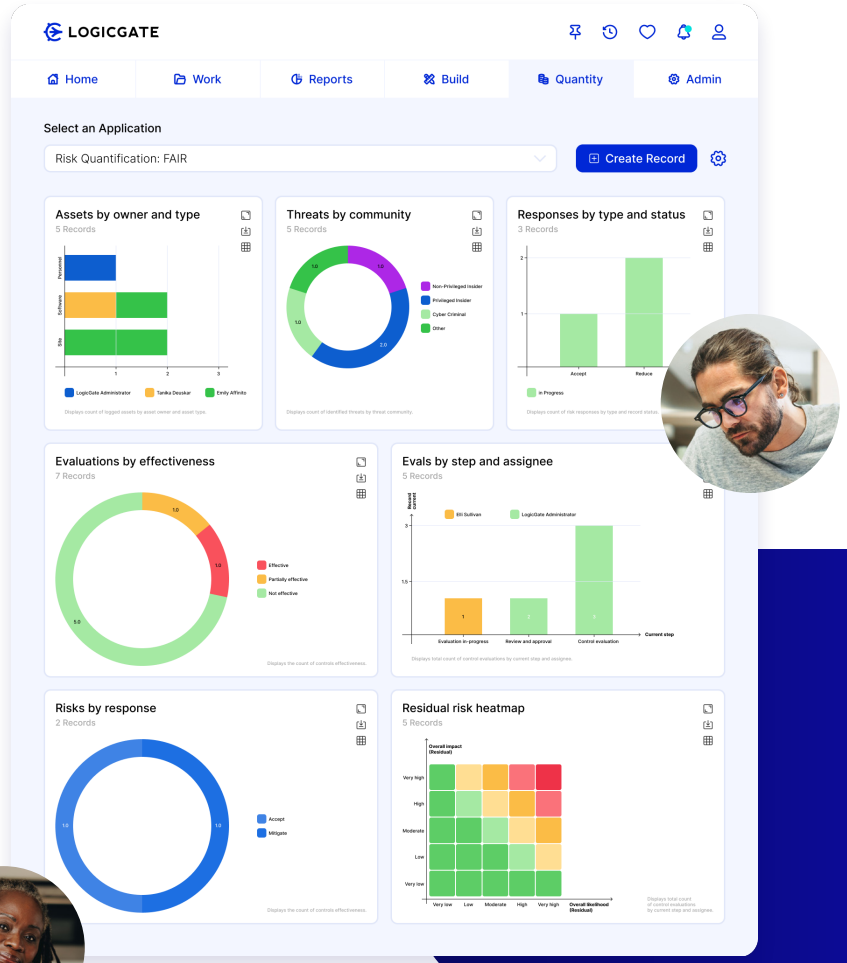
Track the KRIs

Now it's time to map the data associated with your risks, controls, and assets to your preferred KRIs. Implementing an automated GRC platform is one of the fastest ways to accelerate and scale this process as your organization grows.

GRC platforms like Risk Cloud help you dynamically connect and aggregate risk data across every GRC function and business unit. This keeps critical information centralized, up-to-date, and accessible to your key stakeholders with data visualizations and dashboards that align to your KRIs.

While some risk leaders opt to manage their programs manually in spreadsheets – and while it is possible to create and track KRIs in this way – this method carries its own risk. Human error and lagging indicators can quickly erode the benefits of tracking KRIs, as well as your team's ability to mitigate (or leverage!) business risk.

Dashboards built in LogicGate Risk Cloud



Determine risk owners, set thresholds to trigger action, develop action plans

With your KRIs up and running, it's time to position your teams to act on the information they provide as early and as quickly as possible.

For each KRI and its associated risk, assign a risk owner who will be responsible for keeping an eye on the metric and taking appropriate action if the threshold you set for it is exceeded or about to be exceeded. You can also set a series of thresholds for different KRI readings, so that there's a bit more forewarning for risk owners before they get to the maximum threshold.

Think of it like the "check engine" or "maintenance required" lights on your car: Your engine hasn't broken down yet, but there's a good chance there's something wrong with it that should be checked out and addressed.

Start with a threshold target value and use six to 12 months of trending data before creating gated thresholds that prompt specific stakeholder responses or risk mitigation tactics. Starting with set thresholds for new metrics without historical data analysis or proper forecasting can lead to resource waste, or, worse, significantly higher than anticipated risk exposure.

Using risk management or GRC software can help you automate this process by automatically triggering communications to the risk owner when a KRI crosses one of the risk's thresholds.

It's best to report each KRI over a period of time, like quarterly or monthly, to make sure you're able to identify, anticipate, and get ahead of trends. Leadership will also want to see historical data for context during reporting.

Make sure you've deployed controls and developed operational resiliency and business continuity plans for each risk, so there's no chance you'll get caught frantically putting one together while the risk is knocking on your business's door or, worse, is already happening.

If you aren't proactively planning your response for when a risk leads to problems, the work you've done to develop your KRIs could become meaningless. And, leadership will very much want to see that these have been implemented as part of your report.

Reporting with KRIs

While the primary use case for KRIs is to stay ahead of risk trends and keep your organization secure, that's not the only way they can be used. Using KRIs to clearly and confidently communicate your organization's risk exposure and posture to various stakeholders can help you improve your ERM program and get buy-in for new initiatives.

When you're using them in this way, however, it's important to keep your audience in mind. Since department-level stakeholders and risk owners are the ones responsible for responding to and mitigating risks, they will need a significantly higher level of detail than the board of directors or C-suite. In fact, providing top leadership with too much detail can backfire, either confusing them or making it seem like every risk represents a five-alarm fire, even though they do not.

Over-reporting risk in this way can frustrate leaders and actually make it less likely that you'll get their buy-in for your risk initiatives, so make sure you keep things to just the most important information about the most pressing risks. And, it's best to report your metrics visually, in a way they can digest quickly and easily. It shouldn't take an entire slide deck to explain what a metric is and why you're measuring it.

Continuously test and improve KRIs

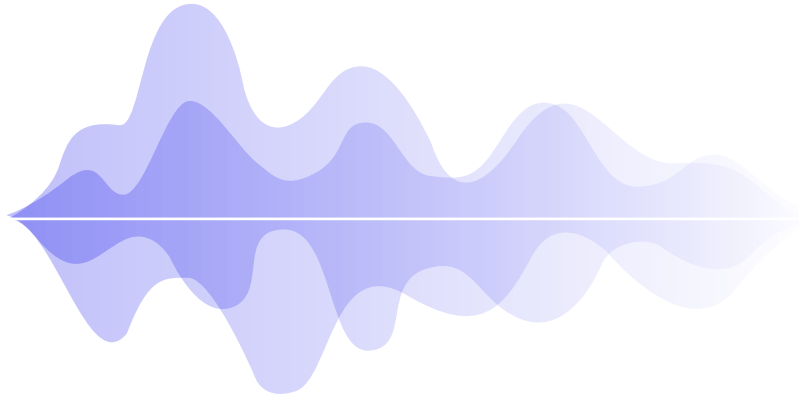
Developing KRIs isn't a "one-and-done" or "set-it-and-forget-it" sort of activity. To ensure your metrics remain useful and continue to help protect your business, you need to be both constantly testing their effectiveness and looking for ways to improve them.

Always be on the lookout for new sources of data that can be used to improve your KRIs or build new ones. New regulatory requirements often lead to increased public reporting of various metrics, and any new business system you bring online can also be a great source of new or more detailed risk data. Whenever you come across this sort of information, look for ways to work it into your risk reporting process.

In addition to tracking your KRIs, you should log every time a risk event one of them is monitoring occurs. If the risk event continues to occur at a high frequency, it's time to reevaluate the KRI tied to it and potentially redesign your method for tracking that risk.

Integrating modern GRC technology and business systems to automate KRI monitoring and reporting

Integrating your other enterprise systems, like vulnerability management and ticketing software, with your GRC platform is a good way to automate the process, streamline data collection, and reduce human input error. This technique allows you to meet the people who are responsible for reporting risk data right where they're at, rather than forcing them to leave the systems they're familiar with to enter the same data into different ones. That can lead to frustration or flat-out refusal. The right integration in the right place makes it possible to have them enter the information once and have it automatically fed into the system that tracks your KRIs.

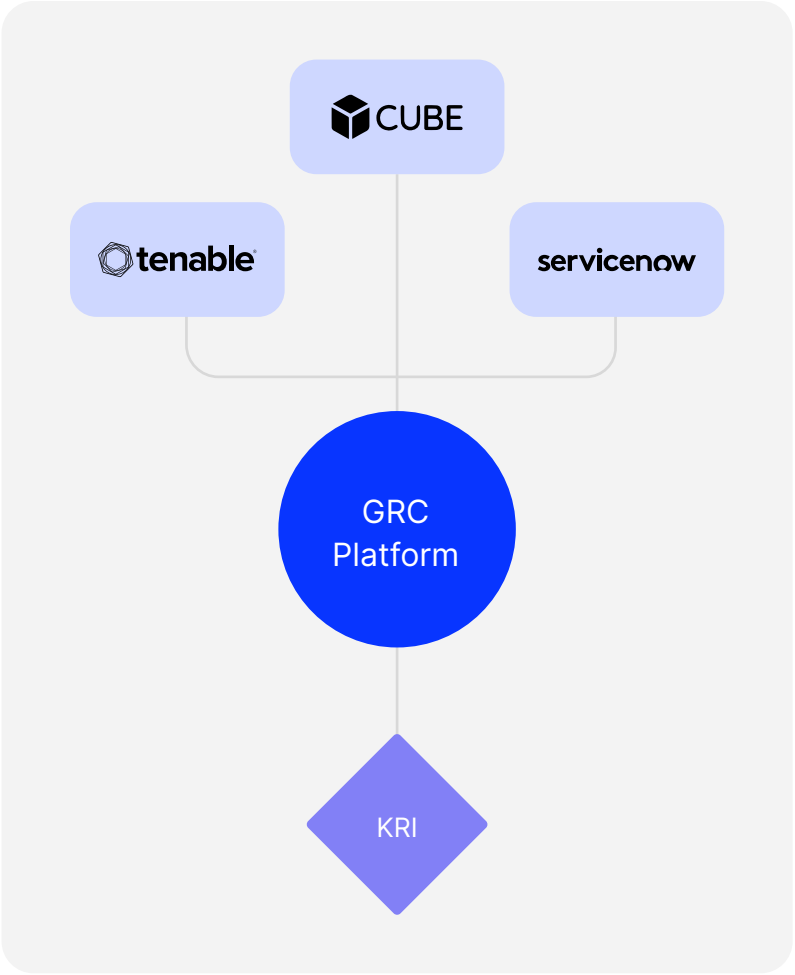


Here are a few examples of what this could look like for your team using LogicGate's Risk Cloud platform:

- **Tenable.io** provides actionable insight into your entire infrastructure's security risks, allowing you to identify, investigate, and prioritize vulnerabilities and misconfigurations in your environment. When used in tandem with Risk Cloud's Vulnerability Management Application, you can quickly and accurately manage the entire vulnerability lifecycle as a part of your broader risk management program.

- **ServiceNow™** helps companies deliver modern, resilient services aligned to customer-centric priorities. Risk Cloud's ServiceNow™ integration connects incident logging from ServiceNow™ to automated workflows within Risk Cloud to simplify response and collaboration. Your team can quickly respond to high-priority incidents from ServiceNow™ according to your internal processes without leaving Risk Cloud.

- **CUBE** is a global RegTech provider empowering regulated financial institutions to meet cross-border compliance challenges head on. When integrated with Risk Cloud's Regulatory Compliance Powered by CUBE Application, you can combine the automation and flexibility from Risk Cloud with intelligent regulatory content recommendations and mappings from CUBE to quickly identify relevant regulations and build an automated, end-to-end regulatory compliance program.



KRIs in the Wild

Now that you have a good understanding of how to develop and use key risk indicators, let's take a look at some examples. Here are 25 common KRIs used across a handful of industries to give you inspiration for building your own metrics specific to the risks your organization is facing:

Economic/Political

1. **Inflation, interest rates, other recession indicators:** Inflation rates and the interest rate hikes that tend to come with them are leading indicators of a potential economic downturn. Tracking these metrics can help you take necessary actions to shore up your business ahead of difficult times.

2. **Employment rates:** Another indicator of economic headwinds, the unemployment rate can provide a heads-up about the likelihood that a drop in consumers' discretionary income will lead to less spending, and thus, lower revenue.

3. **Consumer confidence:** If consumers don't feel good about the direction of the economy, then they're less likely to spend on non-essential goods. Keep an eye on this metric to predict a drop in spending.

4. **Gas and energy prices:** Prices at the pump and rising costs for other commodities used to produce energy can be used as a KRI to predict a variety of economic risks, including a drop in consumer spending and higher costs in your supply chain.

5. **Incidences of civil unrest or conflict:** If protests, armed conflict, and other forms of turmoil are becoming more common in a part of the world that your supply chain depends on, it could be used as an indicator of the likelihood that your supply chain could experience disruptions.

Business/Product

6 

Employee sentiment surveys: If response rates to your employee surveys begin to drop, that can be taken as an indicator that there may be a problem with employee happiness, engagement, or satisfaction in your workforce. This KRI can help you predict and correct talent attrition risks.

7 

Average employee tenure and time to hire: Similarly to employee survey engagement, the average time your new hires spend in their jobs before moving on to another organization or excessively long cycles for hiring new talent can indicate problems with your company culture or discontent in your workforce. Pairing this KRI with the employee survey KRI can provide a heads-up when issues begin to emerge.

8 

Net Promoter Score: While the above two KRIs can reveal problems within your workforce, your net promoter score (NPS) can be used as an indicator of problems within your customer base. An NPS score that is trending consistently down can be the first warning that customers are becoming dissatisfied with your product or services. You can also break this data down by vertical or segment to look for more specific trends.

9 

Reviews and ratings: While NPS is an internally-collected metric, externally-sourced data from reviews and ratings on review sites or app stores can be used for similar purposes.

10 

Net Retained Revenue/churn rate: These metrics are the next step up the risk ladder from NPS and ratings. This is when customers actually start to cancel or choose not to renew their contracts. If net retained revenue begins faltering quarter after quarter, it's time to investigate the causes and get ahead of them.

11 

Number of workplace injuries: If the number of employees being injured on the job at your organization begins ticking up, you can dig into the data by location to tell whether a particular warehouse or office is failing to follow workplace safety protocols and intervene.

12 

Mean time between failure: This is the average time between breakdowns in your business systems, whether it's the digital product you sell or the machinery powering one of your manufacturing centers. It gives you a sense of how reliable your operations are, and when used as a KRI, it can reveal concerning trends in uptime and downtime that may need to be addressed.

13 

Mean time to repair: The sibling of mean time between failure, this metric tracks how long it takes to get your system back online. Longer repairs times mean less reliability.

Banking and Finance

14 

Value at risk: Your value at risk represents the monetary impact your business could experience if your assets were to lose their value over a specific timeframe. Knowing how much is at stake at any given time or in any particular deal can help you make better investment decisions and be sure that you can cover any losses.

15 

Fraud incidents: Tracking incidents of fraud at your organization, whether it's being committed internally or externally, can reveal when there's an uptick in a particular department or other sources, so you can determine where the problem is occurring and fix it.

16 

Loan defaults: If loan defaults begin increasing across the broader economy, being aware of this trend can allow you to take action now to plan for the chance your organization will start to experience large numbers of defaults, too.

Energy and Utilities

17 

Grid/system demand: Electricity, water, internet, and other providers of public utilities track real-time system demand, so that they can implement demand response measures and ensure system reliability during times of peak usage.

18 

Weather forecasts and data: Extreme heat, extreme cold, and other weather events can have big impacts on public utility company operations, so it pays to keep a close eye on the weather. That way, you can plan for any impact severe weather may have on your system.

19 

Government alerts: Government agencies often release data and alerts about threats and incidents that could impact critical infrastructure. Collecting this information and using it to build KRIs can help your organization stay abreast of potential security threats to your assets.

Cybersecurity

20 

Devices under management: The percentage of devices under management by your organization's IT department. The lower the percentage, the most exposure you have to potential cyber attacks.

21 

% MFA: Similar to devices under management, the lower the percentage of employees' devices that have multi-factor authentication enabled, the higher the likelihood you will experience a cybersecurity incident.

22 

% encrypted devices by management group: Tracking the number of devices that are encrypted by department or management group can help you identify outliers, increase outreach and training, and secure their devices before they become a security problem.

23 

Failed phishing attempt simulations: If employees are constantly failing phishing attempt simulations, you know it's time to revamp or increase your cybersecurity training efforts.

24 

High-risk vendor reassessments completed: Your cybersecurity is only as strong as that of the weakest link in your supply chain or vendor ecosystem. The higher the number of high-risk vendors that you're behind on assessing, the greater your risk of a breach.

25 

Mean time to resolve: This is the amount of time a vulnerability exists in production before it's fixed. If your mean time to resolve is going up, it means your patch management is lagging and your organization is more vulnerable.

Conclusion

Access to reams of real-time data has given risk leaders the gift of foresight—an invaluable resource in our line of work. Developing and implementing key risk indicators using the process detailed in this guide will allow you to go beyond what could happen if a risk occurs and start being able to predict when it is about to occur and take proactive steps to prevent adverse outcomes.

That's the power of data-driven enterprise risk management.

LOGICGATE

LogicGate Risk Cloud can help you develop, monitor, and act on key risk indicators to keep your organization secure and turn risk into strategic opportunity.

Schedule a demo today.

320 W Ohio St, Suite 5E,
Chicago, IL 60654
(312) 279-2775
logicgate.com