CENTRL

GUIDE

Practical Guide to Developing Your Key Risk Indicators (KRIs)

Learn how to make effective Key Risk Indicators to protect your business from risks.

US/Global +1 (415) 780 9667 | **UK/Europe** +44 020 3037 8609

And, for more information, please visit: oncentrl.com/vendor360

@oncentrl | /company/centrl/

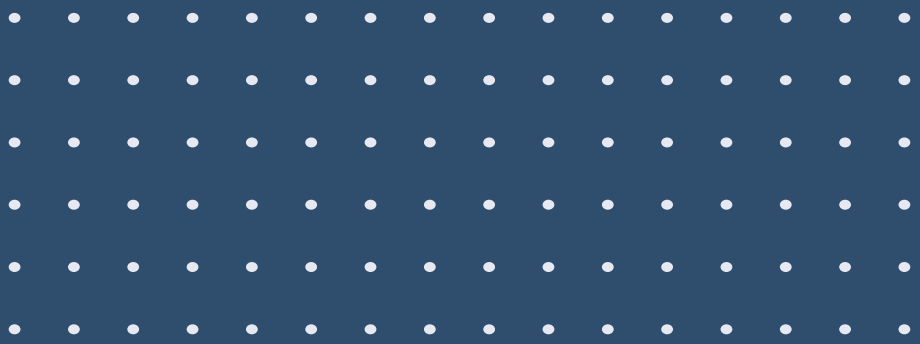
Rev. 2022.7

Introduction

Professionals in risk management, compliance, and internal audit are skilled in identifying strategies to assist firms in managing risk. Processes for identifying and evaluating risks should be iterative and dynamic. Concerning rapidly shifting and complicated situations, auditors must adapt risk assessments, risk responses, and audit methods.

You and your team must create Key Risk Indicators (KRIs) to assist your business units in managing new risks and better preparing for the future. This protects your business from various cybersecurity hazards that might jeopardize its decision-making plans.

These are forward-looking measurements rather than historical metrics. KRIs may be utilized as an early warning system because effective KRIs set thresholds that, when reached, notify management of an elevated likelihood of a future risk occurrence.



CENTRL

What are KRIs, and why are they essential for businesses?

Key performance indicators, often known as KPIs, are measurements created to provide a high-level picture of the company's effectiveness, much like KRIs do. They are an element of the performance management system for the company. Although KRI and KPI are conceptually similar (and occasionally mistaken for being the same thing), they are in fact two distinct measurements.

While both KRIs and KPIs are crucial for benchmarking and achieving corporate goals, they operate in different ways. KPIs monitor and raise a company's output and efficiency. KRIs support KPIs by assisting in monitoring and removing obstacles to KPI achievement. The organization's capacity to achieve the goals that KPIs monitor will be less hampered by employing KRIs to manage risks.

KRIs, in a nutshell, make risk monitoring and management more effortless. A risk indicator is any parameter used to track your risk appetite and exposure over time. They turn into KRIs when they follow a risk that is very significant or do so exceptionally effectively due to their predictive value. Of course, it's best if they carry out both.

If a KRI indicates the potential occurrence of a risk, companies will be able to see which elements of their Risk Management Program are lacking. At the same time, these indicators allow companies to promptly mitigate risks before they impact the organization and prevent the most severe effects of these threats.

CENTRL

Key Risk Indicator Types

Key Risk Indicators keep an eye on threats to a firm's strategic strategy and unique requirements. Therefore KRIs that are useful for one organization might not be the best choice for another.

- **Quantitative KRIs:** These are based on discoveries from mathematical models and analysis techniques and concentrate on verifiable facts and numerical data.

- **Authentic KRIs:** These KRIs put a lot of effort towards foreseeing probability-based outcomes to facilitate sensitivity analysis, for example. It may be more appropriate to utilize quantitative KRIs than qualitative ones depending on the nature of your business or industry. Additionally, depending on internal or external environmental conditions, some KRIs may alter in relevance, rank higher on the priority list, or be given a greater priority than others. Here are some examples of the most popular KRIs utilized in many fields and businesses.

- **Monetary KRIs:** For commercial or retail banks, asset management companies, or Certified Public Accounting (CPA) organizations, quantitative financial KRIs could be more important. Financial KRIs that assess an economic downturn or regulatory changes are two examples of those that might be linked to external environmental conditions. Changes in strategic objectives, budgetary restrictions, or acquisitions are examples of internal influences.

- **KRIs for human resources:** Employing quantitative or qualitative people-based KRIs is likely to be of interest to staffing and recruiting companies as well as human resource departments. Human resource KRIs include things like high staff turnover, low employee satisfaction, labor shortages, or low hiring conversion rates.

- **KRIs for operations:** Operational KRIs might track everything from inefficient internal controls to failed internal processes. All sectors may normally produce these kinds of KRIs. Process inefficiencies, changes in leadership, or adjustments to strategic objectives may all have an influence on operational KRIs.

- **Technology-related KRIs:** Events that are measured by technology-based KRIs include system outages, security lapses, and denial-of-service situations. These KRIs have an effect on many industries, but they may be more significant for a corporation that offers technological services or relies on online business portals. Increased operational complexity, security concerns, modifications to rules or legislation are a few examples of technological risk factors.

How can you develop your own KRIs to suit your specific needs and operations?

One of the essential things that every leadership team is accountable for is performance evaluation and ensuring that objectives and milestones are accomplished. Every day, executives throughout the organization want to see information on their dashboard that informs them of the current situation and, ideally, confirms that they are on track. This information includes KRIs. KRIs are only helpful when built following this rigorous yet straightforward technique. They warn management when they go outside thresholds that there is an elevated possibility for risk exposure.

CENTRL

Find the Right Risks

Understanding your company's goals and any vulnerabilities that may provide risk areas is crucial before implementing KRIs. Finding the most critical potential risks is essential for effective enterprise risk management. These risks are the ones that will have the most considerable effects, have the best chances of happening, or are more likely to be beyond your company's control.

Construct Your KRIs

Key performance indicators (KPIs) your organization has previously created might result in KRIs. Why? The KPIs will already make sense and give the necessary data; this can reduce the amount of time and resources required for monitoring. Remember that the KPIs being converted to KRIs must also be accurate, timely, relevant, and quantifiable. The KPIs shouldn't be utilized if they are outdated or no longer appropriate.

Create a Reliable Process

Each department creates KRIs. Hence a reliable mechanism must be established for developing, evaluating, monitoring, and reporting them to the appropriate parties. The best practices listed below help make sure everything runs well.

- Be sure to include all necessary stakeholders early on while identifying KRIs.
- Obtain stakeholder support, so everyone is invested in the project's success and on the same page.
- Ensure all stakeholders have access to all information on KRIs and the process.
- Establish a centralized point of contact where stakeholders may go for assistance.
- As situations change, promptly inform stakeholders.

By following these guidelines, you can rapidly create an efficient KRI system that supports your organization's strategic objective. Although this is a terrific beginning, you should have a long-term plan to develop your KRIs and the process.

What are some common pitfalls to avoid when creating KRIs?

For a huge percentage of the industry today, risk-based monitoring (RBM) is still a pipe dream; something to strive for but is challenging to accomplish. The process of implementing RBM is complicated and demands knowledge.

The types of challenges range from those that are more business-oriented, like vendor selection and Return On Investment (ROI) demonstration, to operational challenges relating to the site, the on-site monitor, and the central monitor, technology challenges relating to the integration of data from multiple sources and providing customized, scalable, and customizable views, as well as challenges relating to the core science of Risk Based Monitoring (RMB) - understanding how to identify and define Key Risk Indicators (KRIs).

The second challenge is choosing which KRIs to use.

The difficulties associated with the choice of KRIs came in second, closely followed by interpretation. The ideal KRI count is sometimes a difficult one to determine. The concentration and hence the efficiency that RBM is supposed to bring about would be lost if you went too far. On the other hand, omitting crucial KRIs might be extremely harmful because the associated data points could never be evaluated.

The third challenge is how to interpret KRIs.

Finally, your list of KRIs is ready, your triggers are operating, and you are currently looking over a number of fascinating dashboards. Knowing how to properly evaluate the data and connect a firing KRI with the risk impact is vital in this situation. Before analyzing the results and taking any action, one must consider how the KRIs have been set up and which of their respective KRIs needs to be evaluated.

Finding the Best Approach for KRI Calculation

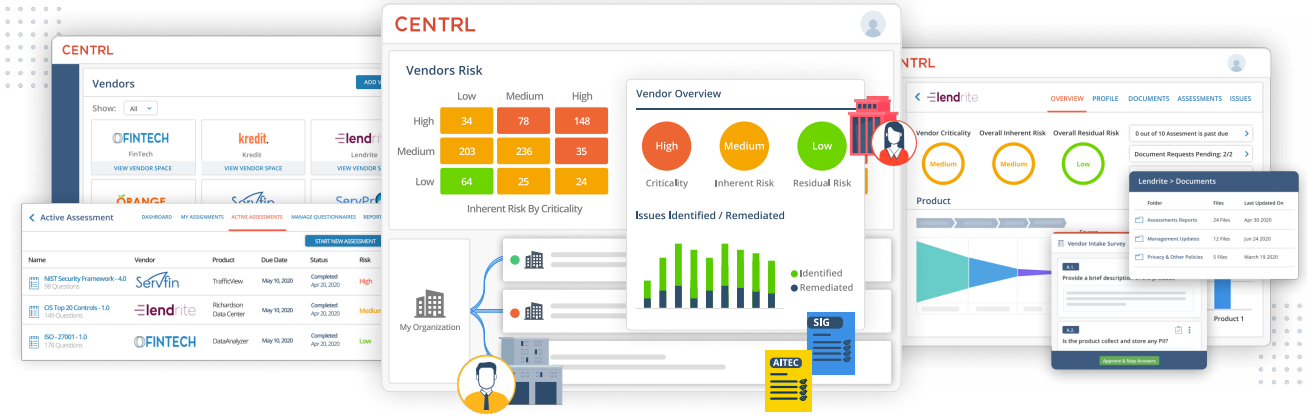
Not surprisingly, a survey taken during a webinar on "Best Practices in Defining KRIs for Clinical Trials" led by Dr. Nimita Limaye (CEO, Nymro Clinical Consulting Services) and Dr. Artem Andrianov (CEO, Cyntegrity) revealed that finding the best method for calculating KRIs was the most significant challenge mentioned by 22% of the participants. For this problem to be addressed, the appropriate mix of clinical and statistical competence is necessary, yet organizations frequently lack the latter.

How should you go about monitoring and reviewing your KRIs on an ongoing basis?

Critical risk indicators should be prioritized and linked to a KPI and a strategic aim to retain the emphasis on the most significant risks. Although the frequency will vary depending on the type of KRI, KRIs must be monitored and recorded regularly.

Professionals in Enterprise Risk Management (ERM) and auditing are crucial in ensuring that the appropriate measurements are in place to limit risk exposure. Utilizing KRIs effectively also depends on having the proper risk management framework.

Establish and develop your KRIs easily with Vendor360



Our third-party and Vendor Risk Management software, Vendor360, incorporates all the benefits of good VRM software, as discussed above. On top of that, it automates the assessment, audit, and monitoring processes, providing you with complete control over the VRM process.

Your vendor management process is made simpler by the Vendor360 System-of-Record, which also collects all vendor management papers and keeps track of all duties from start to finish. As a result, your teams will communicate regarding vendor relations and raise issues with suppliers more efficiently.

The Vendor360, tool that streamlines workflow, shows task managers the dates on which suppliers responded to inquiries and the status of the current assignment.

Vendor360 automated features take care of time-consuming tasks for you, allowing you to concentrate on the overall compliance picture and making your vendor risk management more effective and efficient. To learn more, contact us today.

CENTRL

Learn More: oncentrl.com/vendor360

Get a 1:1 Demo: oncentrl.com/demo-request

US/Global: +1 (415) 780 9667

UK/Europe: +44 020 3037 8609

vendor360@oncentrl.com

/company/centrl

@oncentrl

CENTRL is a leading risk and compliance technology company that provides the most advanced software platform for managing third-party risk and due diligence. CENTRL offers solutions for automating vendor risk management, modern slavery act compliance, due diligence, and bank network management. CENTRL's platform is used by leading companies in all sectors across the globe.

US/Global +1 (415) 780 9667 | **UK/Europe** +44 020 3037 8609

And, for more information, please visit: oncentrl.com/vendor360

@oncentrl | /company/centrl/

Rev. 2022.7