The Power of Key Risk Indicators (KRIs) in Enterprise Risk Management (ERM)
Key Risk Indicators (KRIs) are critical predictors of unfavourable events that can adversely impact organizations. They monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises and mitigate them in time.

KRIs -- independently or in conjunction with other risk environment related data, such as, loss events, assessment outcomes, and issues -- offer considerable insights into the weaknesses within the risk and control environments. They act as metrics of changes in an organization’s risk profile, but given the changing risk landscape, simply establishing them within the corporate protocol may not be enough.

Safeguarding an organization from operational, reputational and other risks, necessitates periodic and regular reviews of these KRIs. This reviewing process also facilitates timely reporting of key risks to the top management. All of this is possible through an in-depth understanding of risks which will enable proper identification, establish appropriate risk indicators, and monitor performance consistently via the Key Performance Indicators (KPIs), while leveraging technology to assist this process.

Characteristic Features of KRIs\(^1\):

KRIs are typically measurable, i.e., they can be quantified in terms of percentages, numbers etc. They are predictable and are often used as early warning signals, while also tracking trends over a period of time. Since they offer useful insights about potential risks that may impact organizational achievements and objectives, KRIs are informative and act as a catalyst for decision making. Considering their importance, it is crucial that they are designed with care.

Designing Effective KRIs

Developing effective KRIs mandates a thorough understanding of organizational objectives and risk-related events that might affect the achievement of those objectives.

If the goal is to increase profits by increasing revenues and decreasing costs, an organization may zero in on strategies to achieve this. But several potential risks may crop up which can impact any one or all of the strategies devised. Mapping key risks to core strategic initiatives allows the management to identify the most critical metrics and monitor their performance. These metrics can help oversee the implementation of core strategic initiatives and reduce chances of disruptions.

While most organizations monitor KRIs that have developed over time, it is essential for these to be regularly evaluated for efficiency and continuously monitored to highlight potential risks. Over time, they must be augmented with new KRIs to meet the dynamic circumstances as newer risks emerge and the older KRIs may be insufficient.

Having subject matter experts vet KRI designs will go a long way in keeping the organization safe. They will be able to shed light on root cause events, stress points, and intermediate events in their units or the processes they supervise. Their supervision may ensure that key risks are not sidelined but are effectively communicated at the right time, rather than after an adverse event has occurred.

Effective KRIs are born out of high quality data used to track a specific risk. The source of this data – internal or external to the organization -- must be reviewed and examined carefully. This will go a long way in determining the KRI to be employed. Sources like trade publications, discussions with customers, employees and members of the supply chain will offer insights into the risks they face that can be harmful to the organization at an enterprise level. Once the data is collated, the approaches taken to measure and standardize KRIs must be uniform for the collated information to be robust and to make the decision process easy.

Relationship between KRIs and KPIs

One of the other most commonly used indicators in corporate governance is the KPIs or Key Performance Indicators. While the KRI is used to indicate potential risks, KPI measure performance. While many organizations use these interchangeably, it is necessary to distinguish between the two. KPIs are typically designed to offer a high-level overview of organizational performance. So while these metrics may not
adequately offer early warning signals of a developing risk, they are important to analyze trends and monitor performance. KRIs highlight just the opposite.

KRIs also help the management understand increasing risk exposures in various areas of the enterprise. At times, they represent key ratios that the management can track as indicators of evolving risks, and potential opportunities, which signal the need for action. Others may be more elaborate and involve the aggregation of several individual risk indicators into a multi-dimensional score about emerging events that may lead to new risks or opportunities.

For example, in the banking sector, a bank may develop a KPI that will include data about defaulters. This KPI may highlight an event that has already occurred – a case where a client defaulted on his payment to the bank as per his loan contract. However, developing a KRI would be more proactive way to indicate loan repayment trends before risk events occur.

To balance risks and opportunities appropriately and to obtain the best possible alignment of performance management and risk management, each KRI should be linked to a KPI. KPIs have long played an essential role in performance management. And one of the most effective ways to link performance and risk management is to integrate risk factors into the company’s performance management tool of choice. By integrating these, a company can measure and monitor performance and risk at the same time, as part of the same process.

Selecting KRIs, Setting Thresholds and Beyond

Being proactive and pre-empting an unfavourable situation from occurring is often possible when the metrics to measure the event are clearly delineated. When selecting KRIs, choose the ones that are measurable, meaningful and predictive. Ensure that they are not too many, else managing them becomes difficult. Select only those that offer concrete information. Once these are determined, organizations should validate trigger levels and thresholds, set these based on their risk appetite and tolerance, or internal acceptance, and implement them after seeking approval from the Board of Directors.

Once the KRIs are in place, they must be tracked regularly – the frequency depends on what the KRI represents. These should be reported to the top management and escalation procedures must be established and communicated to personnel handling these metrics. Not all KRIs have the same levels of escalation, so even if the organization escalates higher in a situation, it is imperative to follow the hierarchy of reporting and not overwhelm the management with too much information.

Challenges

While KRIs help organizations to combat risks and adversities, there are enough reasons behind why KRI monitoring also fails to deliver business benefits:

- Difficulty in identifying KRIs for all risks
- Insufficient focus on the causes of the risks
- Failure to automate the collection of KRI values
- Not using existing KPIs in conjunction with KRIs
- Not associating actions with thresholds

But for each of these challenges, there are remedial recommendations: organizations should start with the key risks and then, expand. They should assign KRIs against each cause. And as many KRIs as possible should be automated to prevent them from becoming stale. Existing KPIs should also be mapped with the KRIs and both should be used to forecast risks. Lastly, associating actions with thresholds goes a long way in synchronizing appropriate thinking when defining thresholds.
Role of Technology in Effectively Measuring and Managing KRIs

Given the advances made by technology today, it is imperative to leverage it to look at different indicators in context of the risk data being collated for an organization. If the organization is already using a risk management system, then it has its risk and control assessment data, issue data, and can combine existing KRIs effectively.

Technology enables the measurement of different risk categories, metrics, and even occurrences. The system is not only for risks, it can also be used for asset classes, objectives, controls, processes, business entities etc. Once these are established, one can define thresholds (such as green, amber and red) – which represent rising and dropping indicators, both critical and non-critical. Reporting and dashboards make it easy to see critical areas for analyses, thresholds – breached or otherwise.

Technology can be used to create a comprehensive story when KRI thresholds escalate. Automating KRIs to give them longer lives, track remedial action when KRIs are escalated, track follow ups – are some of the options available when technology is harnessed. Using technology also makes it easier to explain to regulators the actions performed, and the situations that mandated them, since it leaves an audit trail which reveals these details clearly.

Risk management strategies can also be realized for specific, measurable, relevant and timely actions and responsibilities. Towards this objective, it is essential to understand KRI standards and measurement specifications. Furthermore, it is essential to determine the organization’s analytics providers and the metrics consumers through various tools and resources.

One of the biggest benefits of leveraging technology to manage KRIs is that it does away with manual efforts, which can be time consuming and cumbersome. Technology supports manual and automated data collation methods, enables easy definition of thresholds, and tracks issues and actions for breaches. It provides a single interface to define KRI, KPI, KCI (Key Control Indicators) and risk appetites. It is possible to track metrics for causes, consequences and risks and these are easily accessible to personnel studying these within the organization. It is also easy to relate KRIs, KPIs and KCIs to anything in the organization’s GRC library of content.

Conclusion

Designing and setting up KRIs is critical to a successful ERM process. While the potential advantages of creating an effective set of KRIs has been highlighted, it is equally important to set the design elements and protocols for their proper communication and flow within the sphere of corporate governance.

KRIs in conjunction with the KPIs are deemed to be efficient indicators of not just the potential risks to an organization but also how its different units have been performing. Though the difference is simply in perspectives, an organization benefits far more when examining KPIs using risk lenses. It is believed that harnessing technology and leveraging it will only enhance organizations’ risk management approach and complement existing risk identification methods so as to yield significant benefits.

References


MetricStream is a market leader in enterprise-wide Governance, Risk, Compliance (GRC) and Quality Management Solutions. MetricStream solutions are used by leading global corporations in diverse industries such as Financial Services, Healthcare, Life Sciences, Energy and Utilities, Food, Retail, CPG, Government, Hi-tech and Manufacturing to manage their risk management programs, quality management processes, regulatory and industry-mandated compliance and other corporate governance initiatives.