Key risk indicators as a value driver

How can you proactively monitor risk and, at the same time, demonstrate tangible benefit from the effectiveness of your risk management strategies?

Tom Teixeira, George Simpson, Immanuel Kemp

From safety to cyber-security, successfully managing business risk is becoming increasingly crucial to company survival. How can organizations ensure that they are monitoring risk and the right indicators effectively? The authors provide in-depth advice on how using key risk indicators to drive proactive executive behavior can reduce exposure to risk, improving company performance.

"The increasingly complex, interconnected and global nature of the risks we face demands greater understanding and 'air time' at board level and regular, in-depth discussion with relevant market-facing executive teams."

Sir Peter Gershon, Chairman, National Grid PLC and Tate & Lyle PLC

The risk landscape of the modern business environment is constantly evolving, and companies need to maintain continuous oversight to deal with key risks that could threaten their businesses. Over the past decade, a number of high-profile corporate crises, many directly attributed to failures in risk management, have highlighted the extent of the problem and the danger posed for many organizations now. Notable recent examples include the collapse of UK construction giant Carillion (with contract risk as a key driver), and the cyber attack on shipping and energy company A. P. Moller Maersk. Corporate boards are increasingly demanding the ability to continuously monitor risk exposure, using metrics to assess, validate and verify whether risk is increasing or decreasing.

Meanwhile, executives and other stakeholders need the ability to respond rapidly to emerging threats before these crystallize into serious financial and reputational impact.

This is of particular concern to executives, such as CFOs, general counsel and company secretaries, who in many cases are responsible for ensuring that adequate risk governance is in place. In addition, companies stand to benefit financially by reducing their total cost of risk (TCOR) through reduced insurance premiums, reduced uninsured losses and improved credit ratings. According to the 2017 Aon Risk Maturity Index Insight Report, companies with the best risk management maturity outperformed those with the poorest maturity financially, with up to 15 percent better stock-price performance and up to 25 percent lower stock price volatility. Studies by other organizations, including the Federation of European Risk Management Associations (FERMA), have established similar links between risk management maturity and financial performance.

This article will explore some of the ways in which effective risk management approaches, in particular the use of key risk indicators (KRIs) to drive proactive executive behavior, can reduce unnecessary risk exposure and minimize the potential for catastrophic events. In the sections that follow, we discuss the current state of risk-monitoring maturity in the business world, considerations for the selection of appropriate leading and lagging KRIs, and their effective implementation, and then present insight for executives on what steps to take to improve risk monitoring. While the concepts discussed in this article are well established, evidence shows that management teams are still consistently poor at addressing the process and technical challenges necessary to turn them into fully operational solutions that deliver business value.

Risk monitoring and proactive correction are still immature

Risk management is a growing priority for companies across all sectors, not just those that operate in highly regulated environments. Senior leadership needs to better monitor risk to support improved decision-making, as well as minimize the likelihood of catastrophic events that may cripple their businesses financially and reputationally. This is not a task that individual functions, such as a dedicated risk team, can

manage independently of the rest of the organization. A cross-functional approach at executive level is required for it to be effective. Additionally, there is a growing regulatory obligation for companies to make statutory disclosures on financial viability, solvency and liquidity in light of the key risks they face. There is also pressure exerted by more active investors demanding evidence that risk management is reducing uncertainty and volatility, while improving confidence in financial forecasts.

However, shortfalls in the risk management approaches many companies currently operate can leave them dangerously exposed. These companies either have no corporate-level mechanisms for monitoring and acting on risk exposure, or gather potentially relevant data but fail to develop appropriate metrics to support effective monitoring, control and timely remediation. These metrics can take the form of KRIs, which can be used at all levels of management to provide evidence of the effectiveness of risk management strategies being implemented. Even when companies do employ KRIs, they frequently select inappropriate ones, for example, relying too heavily on lagging indicators rather than leading indicators. Alternatively, they struggle to implement effective monitoring environments that will provide early warning that their risk management strategies are off track, and thus enable timely corrective actions.

The maturity in approach can vary enormously, even though this methodology has existed for some time. Many organizations operate in the first two boxes of the simple maturity model illustrated in Figure 1. Although insufficient KRI-related maturity assessments have been conducted to develop a robust universal benchmark, our experience assessing maturity suggests that most companies, even those conforming to Fortune 500 best practices, lie towards the lower end of the maturity scale, and usually lower than where senior management thinks they are operating.

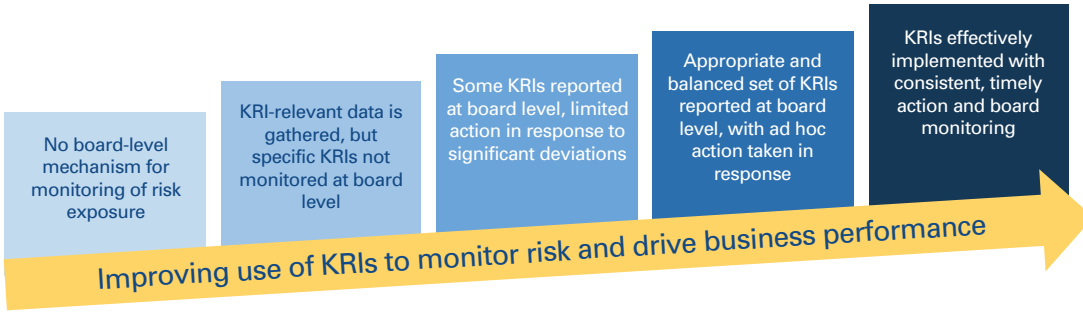

Figure 1: **KRI maturity model**

Selecting key risk indicators

KRI selection is not a trivial or simple process – the characteristics required of effective KRIs are illustrated in Figure 2 below.

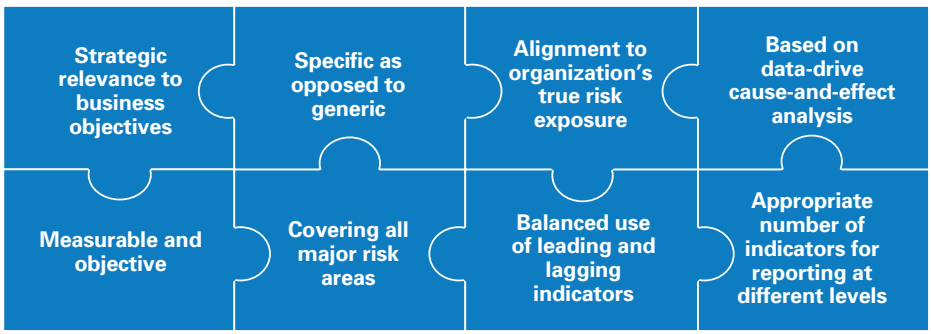

Figure 2: **Characteristics of effective KRIs**

For example, cyber risk might be monitored via 20–25 KRIs within each business unit, while only a few metrics are reported at board level. The challenge lies in developing appropriate board-level KRIs that appropriately capture multiple business unit-level KRIs to give an overall indication of a key risk area, such as data governance or cyber security awareness.

The distinction between leading and lagging indicators is, in our experience, often misunderstood. A lagging indicator is a measurable outcome that informs us about what has already happened, e.g., accident rates. A leading indicator is a predictor of future outcomes – for example, the extent of employee compliance with a company's safety standards may correlate with future accident trends. An effective set of KRIs requires balanced use of both leading and lagging indicators, as they have complementary characteristics, illustrated in Figure 3 below.

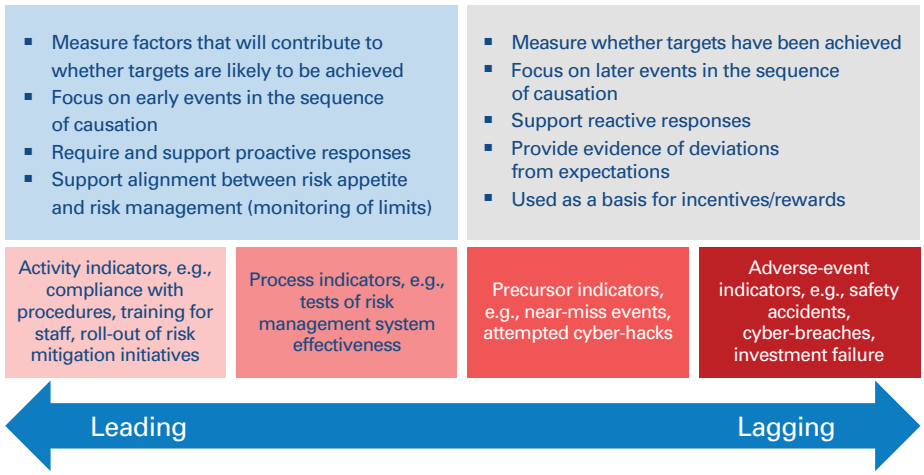

Figure 3: **Leading and lagging indicators**

The distinction between leading and lagging indicators is not a sharp one, but rather a continuum between two extremes based on how close the indicator is to the adverse event in its chain of causation. For example, the frequency of a known precursor to an accident may be used as a risk indicator. This is a leading indicator compared with accident frequency itself, but a lagging indicator compared with compliance with safety procedures that aim to prevent both precursor and accident. Leading indicators must be causally linked to the risks they are being used to measure; i.e., when an indicator improves, the likelihood of an eventual outcome also improves.

The impact of failure to recognize appropriate leading indicators is demonstrated further in the Hatfield case study. (See Box 1.)

Box 1: Lack of leading indicators – The Hatfield rail crash

On October 17, 2000, a train derailed at Hatfield, Hertfordshire, UK, killing four people and injuring over 70. The accident was caused by metal fatigue of the rails, resulting from poor maintenance oversight by the private railway infrastructure company, Railtrack. Due to this, the company went into administration and was replaced by publicly owned Network Rail. From a KRI perspective, we can observe that:

1. *Safety improvements following previous rail accidents at Southall and Paddington had led to **complacency** around the potential for train accidents, which made this event a "black swan".*

2. *Railtrack had failed to recognize the **causal link** between the track defects and a fatal derailment event.*

3. *Railtrack therefore had not been adequately monitoring track defects, which would have served as a **leading KRI** for derailment risk.*

Therefore, the Hatfield crash could be attributed in part to failure to use appropriate KRIs, which allowed Railtrack to be caught unaware by a major accident that ended the company through financial and reputational consequences.

Implementing key risk indicators

Another major reason companies fail to make effective use of KRIs is that while they may select relevant and useful indicators to monitor, and in many cases already possess most of the relevant data, they fall short of implementing systems to monitor and manage them proactively. Implementation is often more of a challenge to get right than the process of identifying and selecting the right KRIs. This is something many boards overlook in favor of simply deciding on a KRI profile and leaving it to the subdivisions of the organization to measure them and report back.

Furthermore, many organizations have failed to commit to full implementation once they understood the complexities and effort required to deploy an effective monitoring environment, citing lack of resources and capital. As mentioned previously, most of the data required to be monitored and interpreted already exists, and the following questions need to be answered, as illustrated in Figure 4 below.

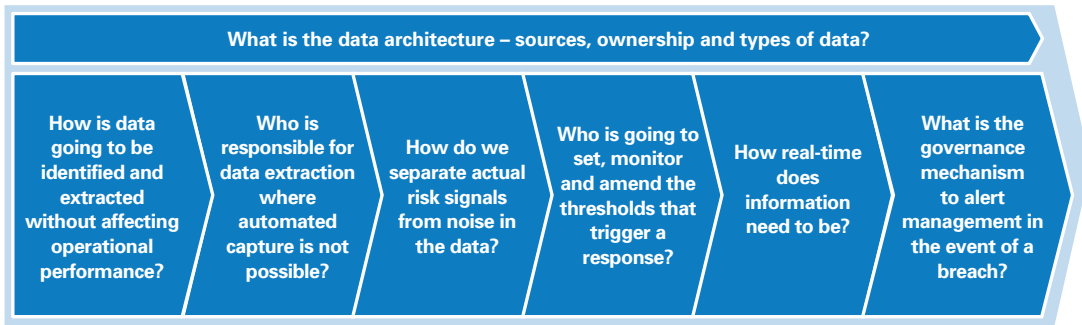

Figure 4: **Considerations for designing an appropriate platform for KRI implementation**

Features of effective KRI implementation should therefore include the following:

- **Appropriate limits** and monitoring for when these are breached.

- **Traffic lights** for assessing the severity of breaches (see Figure 5), with differentiation between "amber" levels, for which closer monitoring is required, and "red", for which senior leadership intervention becomes essential. The "amber" level should represent the organization's risk appetite.

- **A data-driven approach** to determine KRI thresholds and limits, relying on actuarial data as much as possible, rather than pure estimation and a "finger in the air". The "red" limits should represent genuinely high-probability risk (i.e., close to impacting, with significant consequences requiring immediate attention and action) so as to avoid excessively frequent alarms – a situation that tends to breed complacency towards future, more serious breaches. Where robust data is not available (e.g., for various cyber-related scenarios), judgement using subject-matter expertise remains integral in determining appropriate limits.

- **Effective communication processes** for ensuring the right information gets to the right level of management at the right time once a limit has been breached.

- **Selective focus** to avoid the situation in which senior leadership becomes accustomed to excessive "alarms" and begins to disregard them.

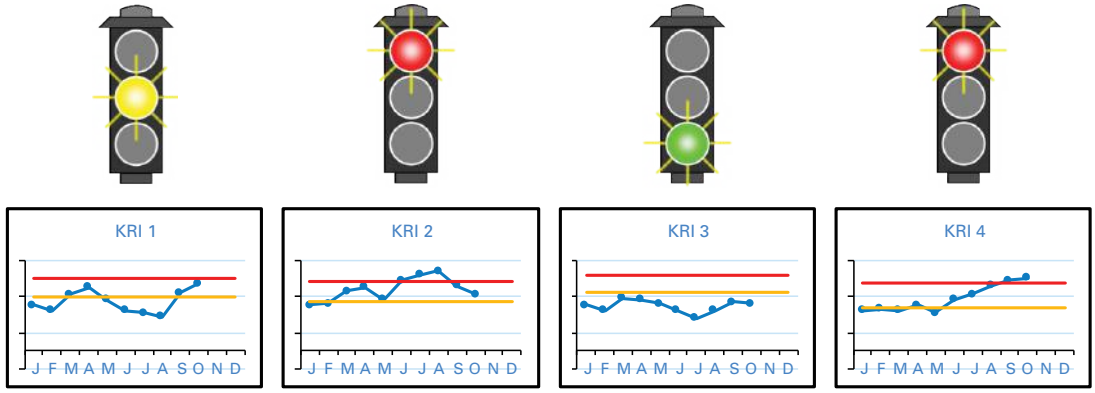

Figure 5: **Illustration of KRI profile (at company-wide or individual business-unit level). Yellow lines represent risk appetite and red lines represent "danger level" with amber and red alerts, respectively**

The importance of senior management performing proper oversight based on robust KRI implementation is further illustrated in the case studies below, on the Texas City Refinery explosion of 2005 and the collapse of Northern Rock in 2012 (Boxes 2 and 3).

Box 2: Robust KRI implementation – BP Texas City, 2005

On March 23, 2005, an explosion occurred at the BP-owned Texas City Refinery, killing 15 workers and injuring over 180 others. The independent Baker Report identified a variety of causal factors:

- *BP had been effectively managing personal safety risk, employing KRIs such as accident rate. However, BP's management of process safety risk (i.e., the risk of releases, explosions, etc.) was poor, and due to over-reliance on personal safety KRIs, managers were unaware of this.*

- *BP had a poor culture of reporting risk upwards within the company, with bad news from safety audits often not reaching senior management.*

- *Cost-cutting decisions by senior management had led to deficiencies in safety management on site, due to lack of awareness of the potential safety risk impact.*

This illustrates the importance of ensuring causal linkage between the KRIs monitored and the risks to be managed, as well as the implications of senior management making decisions in the absence of appropriate risk information. Following the Baker Report, BP undertook a program of improvements to safety management across its five US refineries.

Box 3: Poor reporting culture – Northern Rock, 2012

In 2012, the British financial services provider Northern Rock was forced to nationalize following the first run on a UK bank in over 150 years. This happened after a liquidity crisis in wholesale markets due to the large volume of mortgage defaults in the US, as 70 percent of Northern Rock's funding came from these markets. We make the following observations:

- *Northern Rock had failed to adequately "stress test" its business model.*
- *A **poor reporting culture** was found to have been widespread, with staff tending to under-report mortgage arrears and not challenge management approaches. This poor culture would have been symptomatic of, and contributory to, shortcomings in **management awareness of risk**, creating a vicious cycle of risk-blindness leading up to the event.*

This illustrates the importance of management proactively encouraging appropriate risk reporting to ensure they receive an accurate picture of risk exposure.

Crises such as those affecting BP and Northern Rock are, in part, unpredictable, but the risk can be managed if the right data and events are effectively captured across the organization, stored, processed and visualized to support decision-making and timely correction. In order to consolidate this data into a form that is usable for this purpose, management should consider using digital patterns such as event-driven architectures that:

- Are designed to create insight from data that is locked within existing systems and was previously costly/very difficult to access

- Are visualized through a near-real-time dashboard in a time frame which enables the management team to make a difference to the outcome

- Use consumer commodity and open source technology, which can be implemented faster and significantly more cost effectively than traditional enterprise integration approaches.

A typical corporate arrangement is illustrated in Figure 6 below. This demonstrates how the complexity of a full set of company-wide data necessitates the use of a technology-based platform to process it and issue alerts as close to real time as possible.

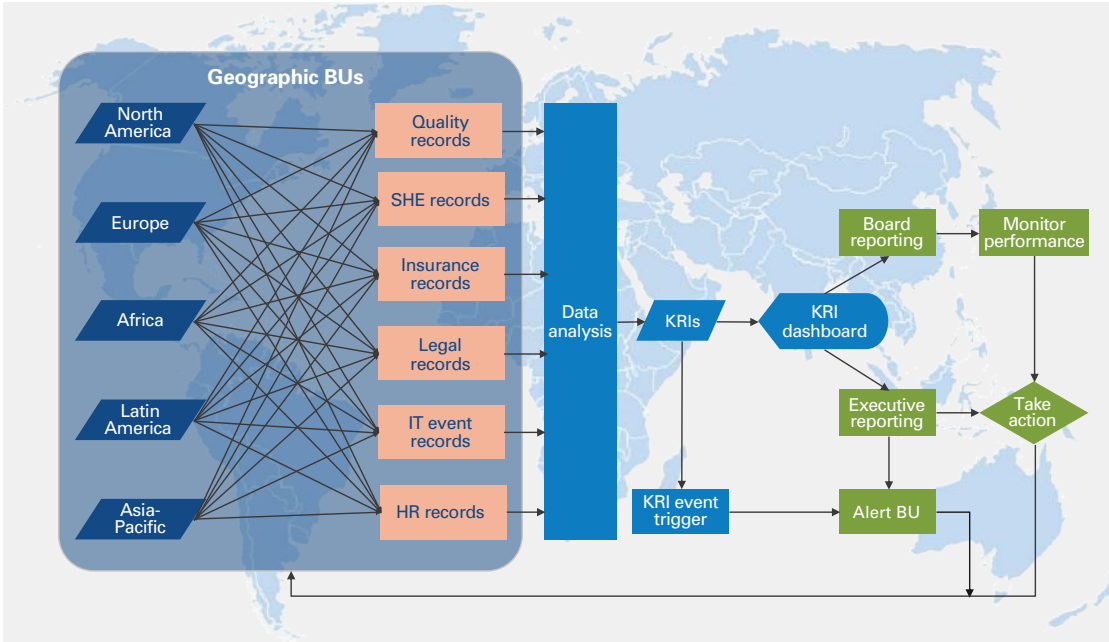

Figure 6: **Complexity related to company-wide collation of KRIs from across business units to drive timely correction and report progress at senior management level**

Insight for the executive

The effective implementation and adoption of KRIs to support improved decision-making and performance improvement can be an involved and complex task for any organization. For risk management to be seen as an effective mechanism for achieving business objectives and delivering the overall corporate strategy, a pragmatic approach should be adopted that balances simplicity with innovative, technology-led solutions. Executives committed to improving risk reporting, getting better understanding of the effectiveness of controls across various operations, and addressing emerging threats early in the process should consider adopting the following steps:

- **Develop (or redevelop) an appropriate, balanced set of KRIs**, ensuring proper alignment to the needs and strategic goals of the business, ease of measurement, and the ability to provide objective evidence of whether key exposures are being effectively dealt with on a timely basis.

- **Determine appropriate, data-driven limits for these KRIs**. Where KRI monitoring has not been implemented previously, a simpler approach with a single limit for each KRI could be considered, with a view to developing a traffic light-system (as in Figure 5) in the longer term.

- **Implement proof of solution (POS) for a number of selected KRIs** to demonstrate the technology solution, define the route to scale across the organization, explore adoption techniques to ensure take-up, and identify benefits resulting from the reporting output.

- **Be prepared to commit time and resources to the development of an effective KRI monitoring environment** – the scale of the task should not be underestimated, but the return on investment is soon achieved through reduced insurance premiums, reduced uninsured losses, reduced risk management costs, and improved credit ratings.

- **Consider the level of detail and format of reporting that will enable effective decision-making**, ensuring that critical information is included while not burdening senior management with excessive detail.

- **Be prepared to use KRI information to inform all levels of management** to ensure that these indicators are used to drive appropriate action. This should prompt timely investigation and intervention at appropriate levels when a risk limit is breached, to avoid adverse financial and reputational impact.

A proactive approach is therefore required for KRI development and implementation with clear sponsorship and commitment at executive level, in order to prevent reversion to a passive risk management approach. It should act as an enabler to drive decisive action to pre-emptively manage risks, reduce TCOR, improve financial performance and provide the right level of board assurance that risk is being taken on a "controlled and informed" basis.

Tom Teixeira
is a Partner at Arthur D. Little's London office and a member of the Global Risk Practice.

George Simpson
is a Manager at Arthur D. Little's Cambridge office and a member of the Global Risk Practice.

Immanuel Kemp
is a Consultant at Arthur D. Little's Cambridge office and a member of the Global Risk Practice.