

## Navigating COVID-19 with Proactive Risk Management

by [Tom Teixeira](#), Senior Consultant, Cutter Consortium

The COVID-19 pandemic has altered the risk landscape for businesses around the globe. Enterprises are learning firsthand whether the business resilience and business continuity plans they put in place are proving successful or not. Moving forward for many organizations, robust analytics supported by technology will be key to accessing data, interpreting it, and deriving relevant insights that will help drive business decisions going forward. Artificial intelligence (AI) and machine learning (ML) tools, in particular, will help identify relevant forward indicators and associated correlations. This technology will set a more “forward-looking” environment based on historical data, and a closed-loop feedback system will ensure new data is ingested on a regular basis, thereby updating the algorithms that have been created and ensuring that the forward-looking risk capability remains relevant to the operating model and environment.

### Facing the Risk

In light of the current, unprecedented global crisis, it's crucial now more than ever to reevaluate your risk management process and ensure you are well prepared for what may lie ahead. Today's executives must adapt their leadership and face the current crisis head-on with a proactive approach to risk management. At its core, proactive risk management is identifying emerging risks early, determining how they should be prioritized, and then responding to them quickly and effectively. The integration of this approach is facilitated by a shift in risk management from a reactive “measure and manage” approach to an anticipatory “sense and respond” approach, which utilizes organization-wide engagement to ensure a dynamic response to risk. This critical need for change follows the evolution of the risk landscape in three fundamental areas:

1. **Era of innovation.** As innovation transforms organizations, technology, and markets, there are ever-changing paths to accomplishing goals, tools with which to achieve them, and developing opportunities for competitive advantage. To ensure value generation, organizations must expand into previously

unexplored business sectors and technologies, thus exposing themselves to a potentially vast array of unfamiliar risks.

2. **Evolving dependencies.** As leading organizations learn to embrace complexity instead of trying to simplify the complicated, they acknowledge increased dependencies: both internal, between business functions, and external, from customers. The consequence of such internal dependencies is that risks that were previously considered immaterial now pose a serious threat across the entire organization. Combining this with increased customer dependencies, wherein society has become accustomed to high-quality, on-demand services, loss of function or reputation can swiftly lead to loss of market share.
3. **Stakeholder expectations.** Increasing scrutiny, from both internal and external sources, means executives are expected to deliver more successful results than ever before. In addition, society places pressure on organizations to accept accountability for any actions perceived to be related to them, ranging from the personal activities of senior leadership members to scandals involving related third parties. This, combined with the viral nature of modern media, means organizations must be seen to respond immediately following an incident or face reputational backlash.

The result of this evolution is that organizations must accept that they are complex rather than complicated. A complicated system is similar to an intricate machine; although the relationships between cause and effect may be difficult to understand, they can ultimately be explained. A complex system is built on the interconnectivity of multiple contributors, meaning these relationships are no longer as definitive and outcomes are not always certain. Thus, executives should accept that their organizations may struggle to fully rationalize or quantify many of the emerging risks they face. However, these risks can still be managed effectively through a proactive approach.

The CEO can now only afford one significant failure, so they must ensure a leadership style that enables their organization to sense and respond to these emerging risks.

## Challenging the Traditional

Traditional enterprise risk management (ERM) is well suited to complicated organizations facing determinant risk. This typically features:

- **Optimized risk management strategy** — a one-size-fits-all approach based on past experiences
- **“Measure and manage” risk approach** — reactive response with separation between risk management and organizational strategy
- **Lengthy internal and public monitoring methods** — risk registers, audit committees, and annual reports

Such ERM approaches can lead to overreliance on conventional methods and discourage the exploration of novel risks and control measures. Even those organizations with exceptional risk management processes may fall foul of emerging risks as they lack the agility to adapt in time. Indeed, the more skilled an organization becomes at managing its known risk profile, the harder it may be to spot weakness or respond quickly to new threats. However, in today's world of rapidly evolving risk, such adaptability is vital. So how do executives equip the complex organization for effective risk response?

## A Proactive Approach

As illustrated in Figure 1, three key aspects are integral to proactive risk management: (1) forward-facing practices, (2) dynamic prioritization, and (3) adaptive response.

### Forward-Facing Practices

As complexity and uncertainty increase, so do the associated risk and the difficulty of identifying this. Predictive risk identification techniques such as horizon scanning and key risk indicator (KRI) monitoring should be used to detect, predict, and monitor emerging risks. Horizon scanning should be undertaken by subject matter experts, with trends analyzed to determine probable futures using political, societal, and organizational data. From this, potential emerging risks can be identified in advance, and effective management strategies put in place.

Once potential risks have been identified, they can be monitored using KRIs, which provide leadership with a real-time health assessment of the organization. KRIs are leading indicators, which are calibrated to provide a “red flag” prior to a risk event occurring; the calibration should be directly related to an organization's risk tolerance. These contrast to key performance indicators (KPIs), which are the traditional,

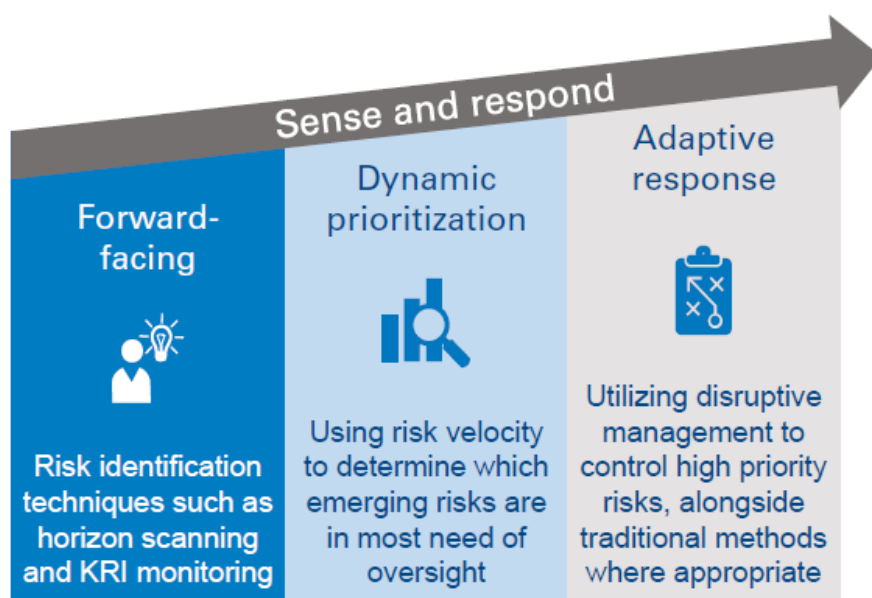


Figure 1 – Three integral aspects of proactive risk management. (Source: Arthur D. Little.)

well-established lagging indicators that provide situational awareness after a risk event has occurred. Such metrics are useful for preventing known risks and recording the performance of control measures, but they do not provide the whole picture.

The holy grail is to have a set of both leading and lagging indicators to support timely intervention to protect the organization and mitigate the risk. KRIs are most effective when detailed understanding of a risk allows informed thresholds to be set. When the threshold is exceeded, an alert can indicate that the probability of a loss has risen considerably, and the risk requires immediate attention. There is even potential for effective KRIs, adequately positioned within the business, to prevent risks from materializing even before those risks have been formally defined. This potential can be realized through AI techniques such as complex-event processing, which enable combinations of data relating to various smaller events to identify larger threats before they manifest.

Furthermore, organizations may expand their forward-facing practices to adopt an anti-fragile approach. This assumes disruption is the norm; therefore, the organization continuously self-disrupts. This is analogous to the biological concept of muscular development requiring stress — the more a system is disrupted, the more it will improve.

## Dynamic Prioritization

Emerging risks are particularly difficult for leadership to prioritize when traditional rating methods rely on severity and likelihood — how can these be gauged when there is no supporting data? A helpful metric here is risk velocity (i.e., how quickly an organization will feel the impact of a risk event occurring). For example, reputational damage due to one-off extremely negative media coverage would be high velocity, whereas changing customer needs as they embrace new preferences would be lower velocity. It is the high-velocity emerging risks that should be given high priority and brought to the attention of the executive.

For such risks, a knowledge base control effectiveness map (see Figure 2) provides an effective reporting tool for executives, as emerging risks can be put in context by relating them to risks with which leadership is familiar. Where velocity is indicated by the size of the marker on the map, it is easy to identify which emerging risks require the highest priority for oversight. The dynamic nature of the map, with risk positions changing on a regular basis, is a more engaging way of presenting risks than the traditional risk register and can be a useful visual tool for executives to use in their working sessions.

Essential to successful risk management today is understanding the varying requirements for different categories or phases of risks. Static risks — which are well understood, have effective control methods, and are unlikely to fluctuate a great deal in the future — are well suited to traditional governance and oversight. Such risks are positioned in the bottom-left quadrant of the map and can be effectively monitored by the risk function.

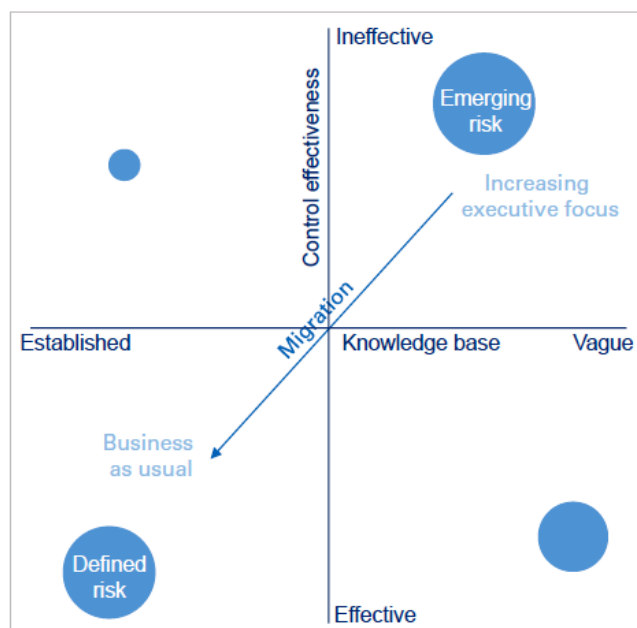


Figure 2 – Knowledge base control effectiveness map. (Source: Arthur D. Little.)

Conversely, high-velocity emerging risks, like those emerging from the COVID-19 pandemic, which are poorly understood and have no controls in place, should be proactively managed through executive oversight and a disruptive management team, as we discuss below. The result should be that, as both understanding and control effectiveness grow, the risk migrates to the bottom-left quadrant. At this point the responsibility of oversight shifts to the risk function.

## Adaptive Response

Adaptive response is the ability of an organization to manage different phases of risk through the most appropriate approach, balancing traditional and proactive methods. One proactive method is disruptive management, which comprises multidisciplinary teams that are able to challenge conventional methods, adapt a project as it develops, and foster a “fail early, learn fast” attitude. The output is achieved through breaking a project into numerous small subprojects known as “sprints,” with proof of concept required at each stage. An adaptive response includes regular meetings for progress updates and to ensure that the response is using an optimal approach. The result is that the end goal is agreed at the project outset; however, the route to get there is not set in stone and may deviate from initial expectations. Using forward-facing practices enables the team to adapt to changing information as understanding of the risk evolves. A reporting tool such as the knowledge base control effectiveness map then provides evidence of success, as teams should observe migration toward the bottom-left quadrant if their approach is effective.

Adaptive response provides an opportunity for executives to swiftly integrate pockets of proactive risk management within the organization and demonstrate its success. This increases the likelihood of stakeholder buy-in and aids setting of the tone for the future risk management strategy. However, it

is important to remember that this approach should be used to complement existing practices, not as a replacement. It is through a combination of the two that organizations can most effectively manage their risk portfolios.

## Conclusion

Executives across the globe are facing unprecedented challenges in managing risk during the current crisis. To respond effectively, organizations must take a proactive approach. Robust analytics supported by technology, including AI and ML, will be key to providing the information necessary to create a more forward-looking environment.

## Acknowledgment

I would like to thank former Arthur D. Little Business Analyst Intern Emily Channon for her assistance and contribution to this *Executive Update*. Ms. Channon has a keen understanding of fundamental risk issues, such as emerging risk management, cybersecurity, and change management.

## About the Author



*Tom Teixeira is a Senior Consultant with Cutter Consortium and an Arthur D. Little Partner. He has more than 20 years' risk management experience, both in senior consulting and operational roles. Mr. Teixeira's key areas of expertise include risk-based strategic planning and forecasting; risk analysis and quantification; total cost of risk (TCOR) reduction strategies, including insurance and captive management; and governance, risk, and compliance technology platforms. He has held senior positions in the professional services and insurance sectors, including EMEA risk advisory partnerships at Alvarez & Marsal LLP and Willis Towers Watson, where he supported FTSE250 and Fortune 500 companies to improve their approach to risk management and drive business performance. Earlier in his career, Mr. Teixeira held the role of Head of Risk Management at Rolls-Royce, the technology company, where he was the recipient of the 2007 European Strategic Risk Discretionary Award for Excellence in Risk Management. He is key author of the AIRMIC's 2017 Risk Appetite Guide; Ensuring Corporate Viability in an Uncertain World, which focuses on the viability statement; the Institute of Directors' 2012 Business Risk: A Practical Guide for Board Members; and contributes regularly to the Wall Street Journal, Financial Times, and Commercial Risks Europe. Mr. Teixeira is a visiting lecturer on risk management methodologies at Cardiff University, Wales. He is a member of British Standards Institute committees for Risk Management and Governance. Mr. Teixeira holds a bachelor of engineering degree in mechanical engineering and energy studies from Cardiff University and a master's of science degree in systems engineering from University College London, UK. He can be reached at [consulting@cutter.com](mailto:consulting@cutter.com).*