Unlike preventable and strategy risks, external risks are beyond an organization’s influence or control. Examples include natural disasters such as the 2010 Iceland volcano eruption, major macroeconomic shifts, and political violence including terrorism. Because organizations cannot prevent such events from occurring, the risk management emphasis is on identifying them, and figuring out through scenario planning and stress testing how best to mitigate their impact in the event they occur.

**first things first**

The first step in managing external risks is to understand the sources of external forces that could influence the viability of an organization’s business strategy. Figure 1 illustrates six major sources of external risks: Political, Economic, Social, Technology, Environment, and Legal. Organizations can begin the risk identification process through considering this classification in one-on-one interviews, surveys or working groups. Cross-functional working groups improve understanding of risks as they facilitate open and explicit discussions. In addition, benchmarking with peer institutions or competitors could provide valuable information on external risks commonly reported in the same industry or sector. It is critical that the Board of Directors approves and regularly reviews the list of external risks to ensure that the consideration of those risks is aligned with the organization’s strategic objectives.

**Figure 1: classification of external risks**

<table>
<thead>
<tr>
<th>Political</th>
<th>Economic</th>
<th>Social</th>
<th>Technological</th>
<th>Environment</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of national or international governance</td>
<td>Failure of a major financial infrastructure or institution</td>
<td>Social instability</td>
<td>Disrupts innovations and new technologies</td>
<td>Major man-made and natural disasters</td>
<td>Changes in tax law</td>
</tr>
<tr>
<td>Interstate conflicts and terrorism</td>
<td>Macroeconomic risks and related market volatility</td>
<td>Massive spread of infectious diseases</td>
<td>Critical infrastructure breakdown</td>
<td>Climate change</td>
<td>Regulatory changes and compliance</td>
</tr>
<tr>
<td>Geopolitical shifts and political instability</td>
<td>High structural unemployment or underemployment</td>
<td>Business and governance corruption</td>
<td>Large-scale cyber attacks</td>
<td>Extreme weather events</td>
<td>Privacy/identity management and information security</td>
</tr>
<tr>
<td>Rising populist sentiments</td>
<td>Fiscal and monetary policy crises</td>
<td>Food and water crises</td>
<td>Massive incident of data fraud</td>
<td>Depletion of critical natural resources</td>
<td>Illicit financial flows</td>
</tr>
</tbody>
</table>

Sources: World Economic Forum 1029 Global Risks Report; Ernst and Young
external risk assessment

Once identified, external risks should be prioritized by performing a risk assessment to help management focus on key risks. Most organizations begin the assessment of external risks with qualitative scenario planning and develop stress-testing capabilities over time for risk scenarios that can be reasonably quantified, if needed in their decision-making process. Indeed, extreme scenarios such as global health pandemics or political changes lend themselves to qualitative assessment and do not necessarily require quantitative models.

It is more common to conduct scenario planning in risk simulation workshops as they improve consideration of risk interactions. Each risk scenario examined by participants should include a definition of the risk events including their drivers, the potential impact of the risk events, and the time to realization of the impact on the organization. Stress-testing helps organizations assess risk scenarios that are worth modeling quantitatively using established probabilistic models. Instead the focus should be on the major changes of one or two specific variables with near-term impact. Financial institutions use stress tests to assess how an event such as the default of a sovereign country would affect their loan portfolios or trading positions.

Once the external risks scenarios have been developed and their impact documented, Enterprise Risk Management (ERM) committees have the responsibilities for reviewing and incorporate them into their business strategy, as frequently as needed. The board can inform management and the ERM personnel about significant trends, outside the organization’s day-to-day operations and industry, that should be considered in the risk scenarios.

mitigation of external risks

The goal of the risk assessment process is not to produce exact predictions. Rather the process is meant to highlight the key exposures to external risks, so that organizations can develop early warning indicators and response plans to mitigate their impact. It is important to create, evaluate and prioritize options for addressing the risk scenarios based on the capabilities of an organization to withstand a risk event in terms of preparedness, agility, and adaptability. While a contingency plan is critical to managing preventable risks, this might be insufficient for external risks events that can manifest suddenly. Companies can be lulled by the illusion of having robust controls and appropriate key risk indicators (KRIs) to monitor exposure thresholds for external risks.

Risk transfer mechanisms from specialized insurers can be used to mitigate the impact of risk events generally excluded from standard hazard insurance policies. This includes catastrophe, cyber risk and political violence insurance. Likewise, financial derivatives contracts are extremely useful to transfer severe impact of an economic variable such as fuel prices to a counterparty. Another possibility is for organizations to exercise real options, decisions made concerning investment opportunities on physical assets. An example of a real option would be the redeployment of a facility currently located in an earthquake-prone area.
The success of an effective and sustainable external risk management program depends upon executives’ commitment in their risk-management function. While a corporate-level ERM function is important, senior management and the board of directors need to be supported by a separate risk-management function to handle external risks, which reports directly to them. This risk function must be performed by people with the right skills supported by technology that is correctly sized for the company.

A large number of Governance, Risk, Compliance (GRC) software vendors provide solutions to build a strong monitoring system for tracking external risks, including real-time dashboards that could be updated automatically with the latest information from commercially or public feeds. In addition to active risk monitoring features, GRC technologies provide scenario management and Monte Carlo Simulation capabilities to assess the impact for selected risks.

Even with heavy investment in technology and training, organizations need to develop risk awareness and mindfulness to cope with external environmental changes in a timely manner, a capability that is seen in High Reliability Organizations (HROs) such as aircraft carriers and nuclear power plants. HROs incorporate external risks into a culture and workforce that respond to threats dynamically. It is only by developing a culture of adaptive capability that organizations could maintain success and performance in an environment where they are continuously impacted by external forces.


**author**

**Famien Konan**

Famien Konan is a Principal Treasury Risk Officer at the African Development Bank with 11 years of experience in the financial services industry. Prior to joining AfDB, he worked at EIB and CNP Assurances in quantitative finance roles. Mr. Konan began his career as a financial software consultant on the credit derivatives markets. He holds a master’s degree in telecommunications engineering from IMT Atlantique (Telecom Bretagne), as well as a mathematical degree from Université de Bretagne-Occidentale. He is a PRM holder since 2010.