Enhancing the identification and response planning for external risks facing today's organizations
Taking risks is an integral part of operating a business. Organizations with more mature risk management practices can outperform their peers financially. Research data\(^1\) shows that financial performance is highly correlated with the level of integration and coordination across risk functions. Creating shareholder returns is the reward for taking and accepting risk, therefore effective management of risk is critical to supporting strategic objectives of the organization.

To succeed in today’s fast-moving business environment, senior executives must take a strategic approach to risk management. Regardless of an organization’s stage of growth, the ability to effectively identify and manage risk is a vital element of success. Companies that are market leaders approach risks intelligently to help them reap benefits and accelerate growth.

Despite improvements in identification, assessment and reporting of enterprise risks, organizations recognize that opportunities still exist to further improve the linkage between risk management and business performance. Boards are challenging whether management is truly engaging in conversations across the organization to identify and assess the risks that could positively or negatively impact an organization.

The first step in creating an effective risk-management system is understanding the types of risks that organizations face. At EY, we distinguish the three key categories of risk: preventable, strategic and external. Each of these risk categories requires a different management approach.

An organization needs to start by identifying and categorizing key risks impacting its business. It should then assess each identified risk to determine its likelihood, potential impact or time to realization. To make the right assessments, organizations need to directly address risk management in strategic and business planning discussions. They also need to routinely evaluate their risk profile and its impact on their business strategy, enabling the organization to readily identify new and emerging risks and adapt their strategy accordingly.

Once an organization has identified and assessed its key risks, it can manage them by designing cost-effective and efficient risk response plans based on the organization’s risk appetite and each risk category.

This insight paper introduces the three key categories of risk and the differences in how each category of risk can be managed. It then focuses and elaborates on the identification and management of the external risks specifically by providing perspectives on the sources of external risks, and presenting an approach on the identification, assessment and management of these risks.

\(^1\) EY “Turning Risk Into Results”, 2012.
Understanding different categories of risks

Preventable risks are internal risks arising within the organization that are controllable and should be eliminated or avoided. These risks present only negative impacts. Examples include business misconduct, regulatory noncompliance, fraud, inaccurate financial statements or errors or defects resulting from breakdowns in operational process. The approach to managing these risks is through active prevention and designing the controls to mitigate these risks. Much of the investment in the controls framework by organizations is driven by preventable risks. The controls framework also provides structured monitoring of the threat level of identified preventable risks.

Strategic risks are risks that offer benefits, risks significant to the organization’s ability to execute its business strategy and achieve its objectives. Strategic risks often focus on the risk opportunity, “there is no return without risk.” Examples of strategic risks include execution of acquisitions and divestitures, new projects development and execution or expansion into emerging markets. Strategic risks are quite different from preventable risks because they are not inherently undesirable. A strategy with high expected returns generally requires the organization to take on significant risks, and effective management of those risks is critical in order to capture the potential gains. Strategic risks cannot be managed through a rules-based controls framework. Instead the approach to managing those risks requires the selection of the right strategic risks to take, improving company’s ability to manage risk events if they occur, establishing risk tolerances, predicting the impact of possible risk events and monitoring key risk indicators (KRIs).

External risks are those that arise from events outside of the organization’s control. These risks can offer negative and/or positive benefits. Organizations cannot influence the likelihood of these risk events, but can reduce the cost of an impact. Examples include natural disasters, political changes, macroeconomic changes including interest rates and exchange rates. Addressing these risks requires a different approach, one that includes identification and mitigation of their impact through scenario analysis and stress testing to determine whether the organization has the minimum resources to weather the full impact of an external risk event.

Companies should tailor their risk-management processes to these different risk categories, and in order to do this effectively it is critical to begin by understanding the three risk categories and developing separate approaches for managing each category. Our 2015 Global Governance, Risk & Compliance (GRC) survey findings reveal that organizations are primarily focused on financial, operational, regulatory and compliance risks, even though many large losses in the market are the result of mismanaged strategic risks and external risks, which include technology shifts, industry disruptions, and the risks of mergers and acquisitions. Because companies cannot prevent such events from occurring, their management must focus on identification and mitigation of their impact.

Leading businesses educate themselves on the implications of external risks, implement steps to monitor and proactively manage these external risks and seek out opportunities to leverage the upside potential of these risks. In taking this approach, leading businesses seize a competitive advantage by engaging with the various unknowns they will encounter and make preparations to actively convert those unknowns into opportunities.

Based on EY’s 2015 Global GRC survey, 85% of organizations indicated there are opportunities to improve the link between risk and business performance.
Risk management concepts

Strategic risks
Strategic risks are those that are significant to the organization’s ability to execute its business strategy and achieve its objectives: strategic risks often focus on the risk opportunity.

Preventable risks
Preventable risks present only negative impacts. These are risks that an organization is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner, as they offer no strategic benefits.

External risks
External risks are those risks beyond the organization’s control: these risks can be unpredictable, as they originate outside of the organization and typically have a low rate of occurrence. External risks can offer negative or positive benefits.

While a compliance-based approach is good for managing preventable risks, it is not the right way to address strategic risks or external risks, which require a different approach based on open and explicit risk discussions. Many organizations apply a generic risk identification process without first understanding the risks embedded in their business strategies.
Here are a few examples of how external events can have a dramatic impact on different businesses

**Legal and compliance: regulation**

As recently as 2012, the US had 104 operating nuclear reactors. With the retirement of Entergy’s Vermont Yankee plant at the end of December 2014, that number has now fallen under 100 for the first time since the 1970s. As many as 10 to 15 additional reactors are at risk of closure – not because they have reached their end-of-life but because of local political opposition and an inability to compete in an electricity market that is vastly changed from what existed when these plants were first conceived, or both.

Look at the example of Exelon in the state of Illinois. Though this state gets electricity from 11 reactors at six plants, three of them – all owned by Exelon – have been identified as the most at-risk because of market pressures: Clinton, Byron and Quad Cities. Exelon officials have blamed the depressed wholesale power prices on high subsidies for renewable energy, especially wind.

On 2 June 2016 Exelon Corporation announced it will move forward to shut down the Clinton and Quad Cities nuclear plants, given the lack of progress on Illinois energy legislation. Quad Cities and Clinton have lost a combined $800m in the past seven years, thanks to cheap natural gas and artificially cheap wind power despite being two of Exelon’s best-performing plants.

Retiring the plants will have a significant economic and environmental impact on the region. The Clinton and Quad Cities plants support approximately 1,500 direct and 4,200 indirect jobs and produce more than $1.2b in economic activity annually. A state report found that closing the plants would increase wholesale energy costs for the region by $439m to $645m annually. The report also found that keeping the plants open would avoid $10b in economic damages associated with higher carbon emissions over 10 years.

**Technological: social media**

There’s no denying that social media has taken the world by storm. Facebook, LinkedIn and Twitter boast millions of users. Social media has become a huge engagement, staffing, retention and (increasingly) branding tool.

Take the example of one domestic airline. On YouTube, you can find a video that one airline passenger posted of a flight attendant singing a country song as part of her opening comments to fellow passengers to “buckle up.” This YouTube video has now been seen by millions of viewers. Think of the marketing and benefits of this example for this airline. A custom on their own, branded the airline’s product in a positive way, resulting in the airline being the beneficiary of millions of views.

Take another example within the airline industry, a well-known customer service case study featuring an international musician. While boarding the flight, a fellow passenger looks out the window after landing and announces to those around him, including the musician, “look at those baggage handlers throwing that poor passenger’s guitar.” Sure enough, the musician’s guitar was broken. Attempting to seek reimbursement from the airline, he faced a mountain of bureaucracy and denials and, ultimately, a rejection. So he decided to take matters into his own hands by simply writing a song and proceeding to upload the video on YouTube. At last count, the video has close to 16m views. The musician has even appeared on national media outlets, released follow up videos, saw an increase in his recording business and even published his first book. The airline ultimately offered an apology, reimbursement and now uses the video as a customer service training opportunity.

Your social media stakeholders include former employees, applicants, customers and clients, vendors, the media and even the government. Social media is the world where Gen Y lives, and if companies want to engage and communicate with this generation, they must embrace social media.
Technological: mobile connectivity
Advances in technological development, especially growth of internet use and proliferation of internet-connected smart mobile devices, have the potential to impact whole industries. When The New York Times Co. purchased the Boston Globe in 1993 for $1.1b ($1.83b today), the price was the highest on record.\(^1\) Still, despite the record price for the Beantown newspaper and some other media properties, it seemed like The Times could still turn a profit on the deal. Then the internet changed the newspaper business, and what was once one of the most valuable newspapers in the world became an albatross around the “Gray Lady’s” neck. After two decades of declining revenue, the Globe and its other New England media properties were sold at a loss for $70m in 2013.\(^1\)

Cybersecurity: digital nature of data
Mining companies increasingly are being targeted by hackers trying to steal information and disrupt operations, as the metals industry expands its dependence on internet-connected systems to reduce costs, according to an EY recent survey. Of the 39 mining companies that responded to the EY 2015 Global Information Security Survey, 41% said they faced a rising number of external threats, including cyber incidents.

Mining companies have tended to focus on the tools of the trade, such as trucks and graters, even though IT has increasingly been used to control that equipment in the past decade, said Mike Elliott, retired Global Mining & Metals leader for EY. “They don’t see themselves like consumer organizations that hold large amounts of credit card details,” Elliott said. “They’re not like a financial institution sitting on large amounts of cash and security. Hence they think they’re not really a target.”

Safety systems and sensors are increasingly being linked to the internet, which has saved mining companies money but created new avenues for attack, the survey found. Mining companies often don’t realize how reliant they are on IT, Elliott said. The mining sector may not have accepted that there are certain “nonnegotiable infrastructure costs” associated with increased dependence on IT. The merging of operations technology with information technology has provided hackers a path to the operation systems from the internet, the report says. The operations systems become “inherently less secure, as many old systems were not developed with security in mind.”

Computer security experts have warned for years that industrial control systems used by utilities, manufacturers and the energy industry are vulnerable to attacks due to buggy software and infrequent patches. Some hackers hunt for information about business deals, while others seek to disrupt the metals markets for profit. Copper is a particularly price-sensitive metal due to tight supply, and the closure of one or two mines can cause its price to spike, Elliott said. Having access to information about those closures before it is made public could therefore be valuable.

---

2. eia.gov/tools/faqs/faq.cfm?id=207&t=3
Limitations in the management of external risks

External risks can threaten the very existence of the organization. All companies are exposed to these risks originating from outside of their direct sphere of influence. However, many companies often struggle to identify them, quantify them or assess their likelihood. Only a few manage external threats with the level of rigor corresponding with the level of impact of these risks. Furthermore, many businesses focus only on certain external risks that seem "obvious," but don’t recognize the full universe of forces that can affect their business.

While organizations have improved risk identification and assessment processes, EY’s 2015 GRC Survey shows executives and boards indicate there are significant opportunities to improve the dialogue around external risks. There are several perceived obstacles to the identification and assessment of external risks:

- Limited resources and time
  - Resources are largely focused on the identification and management of near-term risks, typically operational and regulatory risks
  - Persistent lack of available, quality risk information
  - Lack of reliable information on competitors
- Difficulty determining the scope of external risks to consider
  - Management is often hesitant to openly challenge the strategy, and lacks processes to determine which external risk scenarios should be considered and tested
- Scope and applicability of disruptive forces
- Preconceived notions that external risks are difficult to mitigate in advance
  - External risks are often distant and difficult to put boundaries around. Management focuses their efforts on risks that are easy to capture rather than more distant and less manageable risks

Even with these limitations, there are comprehensive approaches that can help enable organizations to successfully manage the opportunities and the challenges presented by external risks.
Approach to managing external risks

Organizations that methodically identify, assess and respond to external risks that have the potential to impact their business strategy are better equipped to define risk responses that reduce the negative impact of the risk while helping maximize the organization’s potential.

Key to an effective external risk management program is a disciplined approach to assessing all the sources of external risks to which the company is exposed. Without a comprehensive review of all potential sources of external risks, some critical risks may get overlooked.

We identify seven main categories of external risks: political, cybersecurity, social, technological, legal/regulatory compliance, economic and environment (see the graphic below). Organizations can start by identifying key risks that may impact their business by analyzing each of these seven categories of external risks.

Does your business strategy effectively consider external risks?

Case study:

Businesses are specifically asking for an approach to identify and assess external risks, a current void in the marketplace according to EY’s 2015 GRC Survey. In response, EY has developed the External Risk Maturity model to help our clients:

- Gain insights to the external forces and sources that can impact their strategy, mission and vision
- Assess the maturity of their existing management capabilities with regard to identifying, assessing and responding to external risks

Benchmark their external risk maturity against their industry peers

EY used the External Risk Maturity Model to assist a client in assessing its level of external risk management maturity against the seven forces of external risks described above, and benchmark their capabilities against their industry peers. The model provided insights that the company had significant opportunities to improve their external risk management capabilities in the external risk areas of cybersecurity and technology (Exhibit 1).
### Exhibit 1 – External Risk Maturity Model Self-Assessment Overview

<table>
<thead>
<tr>
<th>Leading</th>
<th>Cybersecurity</th>
<th>Social</th>
</tr>
</thead>
</table>
| **Political** | • Proactively analyze interests and engage with both shareholder and external activists  
• Identify and build relationships with political champions and opponents. Advocate for policy approaches that, where possible, address both their interests and yours  
• Develop a holistic political perspective by systematically tracking macro indicators and vetting with well connected local partners and other sources  
• In volatile regions, establish alternative operational measures to employ in the event of unrest | • Cybersecurity seen by C-suite and board as a strategic level risk across all operations and new ventures  
• Has pre-planned and practiced response to breaches  
• Incorporates broader geopolitical, economic, and regulatory issues  
• Cyber risk is linked to individual BUs and their information assets  
• The organization has established and communicated its risk appetite relative to cybersecurity  
• The organization has clearly defined their critical information assets and proactively implements and evolves precautions and countermeasures  
• The organization displays an advanced level of agility and quickly responds to relevant cyber threats  
• Cyber risks are addressed when considering new or evolving technologies | • Structures are flat, collaboration is high, skills in every area (technology, legal, regulatory, etc.) are strategic assets  
• Change is recognized to be ongoing and embraced by the organization  
• Analytics treated as a core capability that creates competitive advantage  
• Impact assessments are common to anticipate socio-economic impacts  
• Social issues are internalized to ensure commitment and consistency to social performance  
• Relationships are built with local communities and governments in which the organization operates |
| **Established** | **Cybersecurity** | **Social** |
| Organization takes actions to cost-effectively reduce the likelihood of occurrence and limit negative effects should the risk event occur. | • Voice given to activists’ concerns, but limited follow through or impact on strategy and operations  
• Work with political allies and advocate based primarily on company interests  
• Outsource political risk analysis with limited local vetting  
• Track conflict and terrorism risks but react only after significant event | • Strong risk management and cyber controls exist  
• Cybersecurity functions are well established and resourced  
• Clear policies and procedures in place  
• Routine stakeholder training on cyber risks and their responsibilities | • A clear picture of potential skills gaps exists.  
• Succession plans exist to close skill gaps  
• The organization is being re-designed for greater agility  
• Change management is thought of early and empowered  
• Effective anti-corruption controls are established and applied consistently across geographies  
• Business continuity strategies are established and communicated |
| **Developing** | **Cybersecurity** | **Social** |
| Capabilities for identifying and responding to external risks exist in pockets, but does not yet yield significant value. | • Activist concerns publically acknowledged but not considered in strategy or operations  
• Political engagement not a priority, conducted through ad hoc personal networks  
• Global political dynamics considered narrowly and based on existing internal knowledge  
• Avoid regions where unrest may affect operations | • Cyber functions are under-resourced with outstanding pockets of weakness  
• Ad-hoc policies and procedures  
• Minimal stakeholder education of cyber risks  
• No consolidated view of digital risks | • Skill gaps exist and informal plans exist to address the gaps  
• Change initiatives focus on training rather than transformation  
• Business continuity plans are incomplete or fragmented across businesses and functions |
<table>
<thead>
<tr>
<th>Technology</th>
<th>Legal/Compliance</th>
<th>Economic</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ IT is being used to create significant competitive advantage</td>
<td>▶ Legal teams have insight into potential regulation changes and provide impact analysis to board of directors on a recurring basis</td>
<td>▶ Assess customer-facing functions and identify areas for measurable improvement in value, effectiveness, efficiency and quality of services delivered</td>
<td>▶ Sustainability committee with representatives from all key areas meet on a recurring basis to confirm qualities that are valued in the physical environment are preserved</td>
</tr>
<tr>
<td>▶ End-to-end integration of enterprise systems</td>
<td>▶ Continuous monitoring of privacy and cyber threats and their monitoring program is reviewed by a third party to assess effectiveness</td>
<td>▶ Identify, where possible, volatility trends and employ counter-cyclical measures to smooth disruptions</td>
<td>▶ Focus on keeping pace with niche competition in maturing market</td>
</tr>
<tr>
<td>▶ Agility to respond to new business demands and innovations</td>
<td>▶ Risk and cybersecurity measures are driving stakeholder trust and the freedom to innovate across the ecosystem</td>
<td>▶ Understand political motivations behind government’s economic actions. Propose a synergistic public-private model that incorporates both political and economic interests</td>
<td>▶ Impact assessments conducted to anticipate impact of climate changes</td>
</tr>
<tr>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td>▶ Tax is involved in all business decisions (at the design phase)</td>
<td>▶ Maintain close communications with local actors and international banks. Diversify investments to allow shifts when needed</td>
<td>▶ Maintain close communications with local environmental boards. Diversify portfolio when needed</td>
</tr>
<tr>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Anticipates evolving policy for taxation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Consumer driven technology capabilities</td>
<td>▶ Policies for terms and conditions, data storage, access and retention are aligned with regulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Capabilities to monitor, detect and respond to social media</td>
<td>▶ Process, governance, monitoring and oversight are in place and effective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td>▶ Impact assessments conducted to anticipate impact of climate changes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Policies for terms and conditions, data storage, access and retention are aligned with regulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Consumer driven technology capabilities</td>
<td>▶ Process, governance, monitoring and oversight are in place and effective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Capabilities to monitor, detect and respond to social media</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td>▶ Impact assessments conducted to anticipate impact of climate changes</td>
<td>▶ Maintain close communications with local environmental boards. Diversify portfolio when needed</td>
</tr>
<tr>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td></td>
</tr>
<tr>
<td>▶ Consumer driven technology capabilities</td>
<td>▶ Process, governance, monitoring and oversight are in place and effective</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td></td>
</tr>
<tr>
<td>▶ Capabilities to monitor, detect and respond to social media</td>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td></td>
</tr>
<tr>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td></td>
</tr>
<tr>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td></td>
</tr>
<tr>
<td>▶ Process, governance, monitoring and oversight are in place and effective</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td></td>
</tr>
<tr>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td></td>
</tr>
<tr>
<td>▶ Process, governance, monitoring and oversight are in place and effective</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Process, governance, monitoring and oversight are in place and effective</td>
<td>▶ Ability to quickly embrace new, disruptive technology fast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▶ Data is accurate, reliable and timely</td>
<td>▶ Consumer driven technology capabilities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Further the client was able to use the peer benchmarking to reach the following insights. Even though their capabilities with regard to both technology and cybersecurity were assessed as “developing,” their maturity within technology was in line with peers but significantly lagging in cybersecurity (Exhibit 2). This initiated a focused alignment of resources to conduct a deeper assessment of their cybersecurity risk program.

Exhibit 2 — External risk maturity benchmark

Practical measures for improving the management of external risks

Identify
Management should first agree on an overall strategic purpose, define what success is to the organization and clarify the underlying assumptions necessary for success. Organizations also need to define what needs to occur (or should continue to occur) to realize the organization’s plan and achieve success. The underlying assumptions also bring into focus the key scenarios that, if realized, could stand to derail the company’s plans. Too many organizations apply a generic risk identification process without first understanding the risks embedded in their business strategies.

After the organization has clarified its strategic purpose and definition of success, the organization needs to consider the origins of external risks, the external forces and the sources of impact that can disrupt its purpose and threaten its success.

An organization can begin the process of identifying external risks through considering the seven major foundations of external risks:

1. Political
2. Cybersecurity
3. Social
4. Technological
5. Legal/regulatory compliance
6. Economic and
7. Environmental

Organizations can benefit from formally brainstorming around each of these sources to consider the disruption scenarios that could impact the viability of their business strategy. For example, technology as an external risk has presented very significant challenges to retailers that have missed the opportunity to adjust their strategy or have been slow to incorporate social media and mobile connectivity into their strategy. The speed of change in the marketplace driven by social media have caused some retailers to lose significant market share, or worse, go out of business entirely.

It is important to include the board in the process of
validation of identified external risks. Management that is engaged in the day-to-day operations of the business may have a difficult time considering the external forces that could disrupt the strategy. However, the board can bring an unbiased and long-term perspective to the consideration of external risks.

Lastly, monitoring competitor activities and assessing competition's publicly reported risk factor statements can provide valuable insights to external risks and provide validation to the completeness of the identified risks.

**Assess**

After the sources of external risks have been identified, the organization needs to assess risk scenarios. Scenarios include a definition of the risk events, the potential impact of the risk events, and the timeframe to realization of the impact and likelihood of the risks occurring. This is accomplished through open and forthright discussions, where participants can speak candidly. The scenarios need to be detailed to help align management to the same risk events.

Scenarios should be developed for the few key risks that could have the greatest impact to the company. If a laundry list of issues is considered, it is possible that little action will result. The assessment needs to bring into focus and highlight the key issues. After the scenarios are developed and the impacts have been considered, the management team should evaluate the external risks against the risk exposures they are willing to accept with respect to the organization’s business strategy. The assessment should be revisited as needed to incorporate changes to the risk landscape or the organization’s business strategy.

**Respond**

Leading organizations incorporate external risks that threaten their viability during the development and maintenance of their long-term business strategy. Organizations need to create and evaluate their options for addressing the risk scenarios and integrate the responses into their business strategy. After options are selected, they should be prioritized based on the timeframe of the risk and effort required to mitigate the risk exposures. Key risk indicators (KRIs) should also be identified and tracked to monitor for changes that could invalidate the strategic assumptions and to provide an opportunity for management to quickly adapt the organization’s business strategy.

Many companies are lacking the maturity to track and periodically assess the seven categories of external risks and apply an appropriate monitoring strategy. Monitoring threat levels for many external risks, for example, may require intensive trend analysis (e.g., social media), tracking of a complex of leading or lagging indicators (e.g., macroeconomic), or qualitative and quantitative business intelligence reporting. Likewise, contingency planning (risk response) for external risks is different than with internal, preventable risks. In part, this is because companies cannot apply preventative controls, they can only respond, so the risk management emphasis is on designing and testing responsive controls. These may include a range of stress-test exercises, including table-tops, quarantines and any number of resiliency plans, such as rapid deployment of assets, capabilities, lines of credit and so forth.

---

**Advanced strategic thinking**

- **Purpose**
- **Business startegy**
- **Risk appetite**

**What risks impact our business?** – Identify risks

**Disruptive forces creating risk and driving change**

Social  |  Environmental  |  Legal  |  Political  |  Technological  |  Economic

**Risk**

**Are they relevant?** – Assess risks

- **Strategic risks**
- **Preventable risks**
- **External risks**

**What do I do about it?** – Respond

*Insights on governance, risk and compliance – External risks* | 13
Managing external risks with GRC technologies

GRC technologies are typically used to manage information within the direct control of an organization. A powerful addition to a GRC ecosystem is the capability to organize and report on external risks, those outside of the organization's control. We are introducing below a few examples of data sources for external risks that can be used in a GRC environment. These sources are either commercially available from a third party or analytically obtainable by an organization.

GRC configuration

GRC software is typically configured by establishing a process, risk and control (PRC) library. The PRC life cycle is relatively static once established, and almost everything in it follows a common routine.

An external risk requires a bit more thought than the known universe of things in the PRC. External risks may not always directly correlate to the relatively static PRC, may be based on theories, models or predictions, and may change with a frequency no PRC owner would want to work with. Organizations can therefore find themselves having to think through how to configure the GRC software to monitor external risks:

1. Many external risks correlate to controls. The cost of oil is a good example of external risk data that can be fed into the system and compared to a KPI for a control. When a threshold is breached, and issue is created, some process is followed, etc. The same could be said for interest rates, the foreign exchange rates, the hourly cost of labor in a specific region, etc. While these types of risks are not controllable by the organization, they are easy to obtain and compute.

2. Many external risks do not correlate to controls, at least not in the traditional sense. The NTAS (National Terrorism Advisory System) rating is an unlikely find in a corporate PRC, yet many organizations that manage disaster recovery with a GRC have some provision in the plan for an NTAS Imminent category, particularly when geographic information is provided with the alert. A feed from the NTAS system into a GRC could serve to automatically generate the first steps of a disaster recovery workflow plan.

Examples of use

Technological: social media

Social media analytics have become commonplace, and many organizations have some capability to perform the analytics internally. Utilizing the output from TIBCO, Tableau, Watson, etc., organizations can determine what represents risk to the organization, establish within the GRC the appropriate controls and KRIs and feed output from these systems into the GRC.

Legal: changes in laws and regulations

Many GRC vendors provide regulatory feed interfacing and access to commercially available feeds as a standard (paid) offering. This feature is rarely implemented (unfortunately).

Political: conflicts and terrorism

Terrorism and global unrest are commonplace events that are reported on a daily basis through email and RSS feeds from organizations such as ISH. Terrorism notification systems, such as the US NTAS system or Britain's MIS, can be set to feed GRC technology with the geography-specific location of terrorist threats. Numerous other systems exist, from local police, FBI, government, regional, Interpol, etc.

Environment: weather and climate change

Tracking weather-related events in a GRC system may seem far-fetched, but the potential impact of a significant weather event may be tied to numerous physical controls. A sudden change in the categorization of a hurricane may necessitate a change from a primary to secondary data center. The controls governing the change are measured in the GRC – a system that can be configured to receive and interpret feeds from NOAA and other sources. Through use of an automated feed the GRC can initiate the workflow required of the first line of defense during the event and maintain data for review by the second line.

Legal: regulation and compliance

Many controls in a PRC exist to meet a regulatory or compliance need. Association of these controls with commercial data feeds can prompt control owners of changes.

Social: public health

Public services such as the US CDC and EU CDPC provide numerous public health feeds that may contain valuable data in risk management systems. Where health and risk intersect, such as the impact of a recall on a supplier or the capability to travel to a region struggling with disease, these feeds can interface with GRC systems and provide alerts, create issues, route tasks, and update controls and risks.
Summary

Different categories of risk require different approaches to how organizations manage these risks. While preventable risks can be effectively managed through a rules-based controls framework, this approach is not suitable for external risks that are outside of company’s control. Businesses are continuously impacted by external disruptive forces and global megatrends. The key to effective management of external risks is to periodically perform a comprehensive assessment across the full breadth of forces and sources of these risks. Once key external risks have been identified, organizations need to be diligent about effectively building resiliency (response capacity) to mitigate these risks in the event they occur. It is critical to build a strong monitoring system to track these critical external risks so that organizations can anticipate these risks and adjust their business strategies to drive performance and sustained success.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2017 EYGM Limited.
All Rights Reserved.

EYG no. XXXXXXX
BMC Agency
GA 1005130

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com