Investments in resiliency will go up as companies seek growth and manage risks

Weeks before the 2020 US presidential election, risk management leaders see eye to eye with other C-suite leaders on the major policy issues facing their companies. Over half of risk and other functional leaders expect post-election tax law changes to have the biggest impact, followed by COVID-19-related stimulus policies (more than 40%). Healthcare policy and US-China trade relations are important policy areas for about a third of all business leaders, including risk leaders.

During the pandemic, functional leaders have encountered similar challenges as they made decisions, designing and implementing their pandemic response. For example, with remote work and accelerated digitization, operations and HR leaders are even more likely to watch for changes to cybersecurity and privacy policy (38% and 37% respectively) than risk leaders (31%). Regardless of the election outcome, risk leaders expect to make greater investments in both risk management and resiliency programs. Closer ties between risk and resilience will help businesses respond better to changes and emerge stronger after a disruption.

Thinking of the upcoming US general election, where would changes in the following policies have the most impact on your company?

<table>
<thead>
<tr>
<th>Policy Area</th>
<th>All leaders</th>
<th>Risk management leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>US tax policy</td>
<td>56%</td>
<td>55%</td>
</tr>
<tr>
<td>COVID-19-related stimulus policies</td>
<td>42%</td>
<td>47%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>31%</td>
<td>34%</td>
</tr>
<tr>
<td>International tax policy</td>
<td>26%</td>
<td>35%</td>
</tr>
<tr>
<td>Cybersecurity and privacy policies</td>
<td>27%</td>
<td>31%</td>
</tr>
<tr>
<td>US-China trade relations</td>
<td>33%</td>
<td>30%</td>
</tr>
<tr>
<td>Environmental policies</td>
<td>21%</td>
<td>23%</td>
</tr>
<tr>
<td>Immigration policy</td>
<td>16%</td>
<td>12%</td>
</tr>
<tr>
<td>Other US trade relations (e.g., Mexico, EU)</td>
<td>11%</td>
<td>4%</td>
</tr>
<tr>
<td>Policy changes would not affect my company</td>
<td>1%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Q: Thinking of the upcoming US general election, where would changes in the following policies have the most impact on your company?

Highest-ranked choices from a list of 10 options.
Source: PwC Pulse Survey
September 3, 2020: All leaders base of 578; Risk management leaders base of 77
Top findings

Seventy-seven risk management leaders (chief risk officers, chief information security officers, and chief audit executives) from Fortune 1000 and private companies, along with other C-suite executives, weighed in on this and other policy-related issues in our latest PwC Pulse Survey, fielded August 28, 2020, to September 3, 2020. Find these insights in our Road to Election 2020 report. In the ongoing survey, risk management leaders also shared their perspectives on other top-of-mind issues, including how enterprise resiliency programs are evolving to meet new stresses, which emerging risks are on their radar and where they’re investing for resilience by design.

Which of the following statements, if any, best describe your current enterprise resiliency program?

- Undefined and ad hoc
- Defined, but not formalized
- Formal and standardized
- Optimized

Risk management leaders

- Undefined and ad hoc: 9%
- Defined, but not formalized: 40%
- Optimized: 48%

Q: Which of the following statements, if any, best describe your current enterprise resiliency program?

Source: PwC Pulse Survey
September 3, 2020: Risk management leaders base of 77

Resilient enough? Risk leaders may be overconfident

As companies respond to the ongoing turbulence, they are confident in their enterprise resiliency programs with most saying they have formalized and standardized—and even optimized—their programs. Driving the overall results are risk leader respondents in financial services (26% of sample), where resiliency has been emphasized by industry players and regulators.

But as they look to what comes next, do they have what it takes to weather future shocks? Risk leaders, in particular, are bracing themselves for more setbacks. For example, 67% of the risk leaders surveyed expect revenue declines over the next 12 months while only 23% expect increases. In the coming months, companies will have to adjust quickly to changes. Some are of their own making as they take on ambitious growth and recovery plans. Other changes are outside of their control: the outcome of the 2020 US election, new waves of COVID-19 infections, heightened cyber threat activity, second-order effects of the global economic downturn on jobs and trade, forecasted severe hurricane season, and resurgent social upheavals.

In this environment, companies need to take an expanded view of enterprise resilience and ask:

- Is the resiliency program connected to the risk management activities and strategy?
- Is there a clear owner of the enterprise resilience responsibility?
- Is there governance around how functions responsible for business continuity, disaster recovery and crisis management should work together?
- Is there a system for communicating status and responses to all the stakeholders, from the boards to the CEOs to suppliers and customers, about the organization’s ability to weather oncoming disruptions?
- Is the enterprise resilience program enabled through technology and truly sustainable with transparency around ongoing maintenance?

In short, companies will need to shift away from fragmented business continuity and disaster recovery responses toward building resilience throughout the enterprise.
Plenty of activities, but are they coordinated?

Companies may overestimate their resilience, in part, because having basic components of an enterprise risk management program may offer a false sense of security. They’ve identified risks facing the business and have a plan for each of them. More than three-quarters of companies, for example, believe they understand risks associated with the large-scale shift to remote working. And 69% say they are managing the resiliency risks related to managing suppliers and third-party relationships.

Where they fall short is in connecting risk programs and activities to their resilience strategy.

Our 2019 study of resilience in more than 3,000 organizations around the world illustrates the disconnect between risk management and resilience.

• Incomplete visibility into core processes and dependencies: An enterprise can’t know which systems or assets to isolate when a disruption occurs unless it has visibility into core processes, assets and dependencies. Among the companies that scored highly on resilience measures, or the high Resilient-Quotient (high-RQ) group in our study, 91% maintained an accurate inventory of assets at any given time. Only 47% of the rest of the respondents did so.

According to a preview of the results of a three-day simulation of real-world events called Cyber Storm 2020 in August 2020, many companies and government agencies still don’t know the full extent of their dependence on contractors and other service providers.

• Inconsistent understanding of impact tolerance: Another weakness lies in defining and testing how well an organization can stand up to disruptions. About two-thirds of high-RQ respondents have set impact tolerances for critical business services, while only 24% of the rest of the survey respondents have done so. Routinely, these impact tolerances do not uniformly apply to both businesses’ view of criticality and their IT counterparts.

The recent surge in ransomware attacks underlines the importance of this. With no time to waste after an attack, an organization must rely on its predefined limits on the nature, severity and length of disruption it can endure, in addition to other risk considerations to help decide whether to pay the ransom.

What's inside your enterprise resiliency program?

<table>
<thead>
<tr>
<th>Element</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic, operational and financial business objectives</td>
<td>78%</td>
</tr>
<tr>
<td>Risks associated with a large percentage of employees working remotely</td>
<td>78%</td>
</tr>
<tr>
<td>Risks associated with managing suppliers and other third-party relationships</td>
<td>69%</td>
</tr>
<tr>
<td>Risk appetite and tolerances set throughout the organization</td>
<td>66%</td>
</tr>
<tr>
<td>Inherent risk management capabilities</td>
<td>56%</td>
</tr>
</tbody>
</table>

Q: Which of the following elements does your current enterprise resiliency program include?

Source: PwC Pulse Survey
September 3, 2020: Risk management leaders base of 77
Resilient by design

Eighty-seven percent of risk leaders plan to increase their investments in resiliency programs over the next 12 months. No matter what the outcome of the 2020 elections is, risk leaders and other executives are more likely to invest in risk management and digital transformation activities.

To become more resilient, organizations need to bring together interrelated capabilities—risk, compliance, business continuity, crisis management, cybersecurity and business operations. Even individually excellent functional teams need to be pulled together to strengthen organizational ability to adapt to changing conditions and emerge stronger after each disruption.

How enterprise resiliency investment is changing

Q: How much, if at all, are you planning to change investment in your enterprise resiliency program over the next 12 months?

Source: PwC Pulse Survey
September 3, 2020: Risk management leaders base of 77
The six steps towards enterprise resilience

- **Establish accountability.** Name the owner(s) of enterprise resilience and the functions whose work need to be coordinated. Depending on the magnitude and velocity of changes, consider standing up a formal resilience function and naming a chief resilience officer.

- **Design the operating model for enterprise resilience.** Determine the infrastructure you need, from assessments through testing, to design the model that supports your organization’s business objectives.

- **Stand up a governance process.** Your formal governance process should define roles and responsibilities, especially from a line of defense perspective. Establish a governance body to oversee interaction and engagement among various teams in the lines of business, security, business continuity, and so on.

- **Align risk management to the resilience strategy.** Develop a harmonized view of the risks with high impact on your organization’s resilience. Apply a strategic lens to tie these resilience risks to everyday risk management and monitoring activities to help identify emerging micro risks that may have significant impact on business and IT operations. Use current reporting mechanisms to show accountability for resilience to the board.

- **Modernize capabilities.** Use technology to ramp up capabilities at lower cost. Platforms like Terrain Insights use automation, analytics and visualization for an always-current view of critical business services and the underlying IT assets.

- **Track progress on your resilience journey.** Use KPIs to monitor: Are we stronger after a disruption? How are we improving the speed—of response, of return to a good state and of learning loops? How is our progress in lowering costs and losses?

Begin your shift away from fragmented business continuity and disaster recovery responses and build resilience throughout the enterprise.
Latest findings: Road to election 2020

No matter who occupies the White House next, business leaders must anticipate what policy and regulatory shifts will mean. The election focuses on big issues, such as economic stability, the role of government programs in driving economic recovery, and responsibility of business in creating domestic jobs and championing diversity and inclusion. See what’s top of mind and keep up with perspectives on how your company can be more agile and responsive to whatever comes next.

Learn more

Current and past surveys

PwC Pulse—September 2020
Workforce Pulse—July 2020
CFO Pulse—June 2020