The future of risk: 5 trends to watch in 2019

2019 may be a pivotal year for many middle market companies from an economic and risk perspective, as growth slows and a new set of risks becomes more prevalent. With these challenges in mind, many companies will face key decisions about how to adjust operations to a rapidly evolving business environment.

RSM’s recent 2019 Economic and Risk Outlook webcast provided key insight into several economic and risk trends. Economic growth is decelerating, as we project 2.2 percent overall growth in 2019, mainly due to the receding effects of the 2017 tax cuts. Beyond this year, we see long-term growth slipping to 1.8 percent, mainly due to slowing household consumption and weak business outlays on capital expenditures.

Some of the resistance to investing in capital expenditures is tied to risk aversion from the Great Recession and the fear of taking on debt for large expenses. While we do see a 21 percent chance of a recession in the medium to long term, this event is unlikely to match the impact of the economic downfall of 2007–2009. Even if a recession does occur, it will likely resemble the telecom or dot-com bubble, with financial struggles limited to a specific industry or region.

The U.S. labor market is currently robust, as we see job creation in 2019 averaging 155,000 per month. We also see the unemployment rate heading to 3.4 percent and wage growth trending to near 4 percent at the outset of 2020. Recruitment and retaining skilled talent continues to be a key stressor for middle market companies, as there is less than one unemployed individual per job opening.

Along with these economic challenges, the risks to middle market organizations are constantly evolving, and 2019 is proving to be no exception. Companies are currently feeling significant pressure in several directions, from global political tensions and technology threats to new data privacy demands. In particular, the following are the five most prevalent risks that you should evaluate and address to help better position your company for success in 2019 and beyond:

1. Volatility and global supply chain

   The global climate can change quickly, as the world is arguably in a more volatile state now than at any time in the past decade. For example, populist and more radical governments are enjoying electoral success around the world, with nationalist and immigration debates becoming increasingly common. The majority of middle market companies have overseas interests, and disintegrating global alliances, tariff wars, cyber wars, terrorism and the rise in the number of natural disasters all threaten the global trade network. The potential impacts include:
   - Loss of key global supply
   - Increased financial exposure
   - Disruption along transportation routes
   - Loss of margin due to short-term supplier switching

   To help mitigate these risks to the global supply chain, you should first review supply chain strategies, identifying potential disruptions and examining alternate solutions. Leading organizations are scenario planning, identifying situations to test response strategies and backup plans. In addition, implementing key risk indicators for vulnerable points and building monitoring dashboards can highlight early signs of problems before they become major issues. Finally, incident response and disaster recovery plans must be updated to incorporate supply chain resiliency.
2. Culture and conduct

People generally do the right thing, but it’s hard to ignore the number of high-profile executives and public figures highlighted for behaving in ways that are inconsistent with corporate values, ethics and even the law. Despite efforts to improve corporate governance, and extensive time and energy spent to improve controls, bad things continue to happen and can spread, subsequently damaging organizations and their value. Potential threats include:

- Loss of reputation and diminution of brand
- Loss of market trust, customers and revenue
- Regulatory breach and corresponding penalties
- Fraud and misappropriation

In an effort to assess your culture and conduct, start by gathering information, identifying strengths and weaknesses, and building procedures to monitor progress, including follow-up surveys. Any findings of culture and conduct analysis can be tied to the role of internal audit, thereby enabling the function to take the temperature of these risks moving forward. In addition, advanced technology tools such as artificial intelligence and machine learning can utilize volumes of existing data to create predictive analytics or identify issues early on.

Of course, established and enforced conduct guidelines can go a long way to discourage unethical behavior. However, over half of the attendees in RSM’s webcast identified having procedures in place, but not knowing if they are sufficient to identify potential harmful behavior.

<table>
<thead>
<tr>
<th>How well do your organization's procedures identify and manage conduct risk?</th>
<th>53.2%</th>
<th>24.8%</th>
<th>12.5%</th>
<th>9.5%</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have procedures in place but we are not sure if they are sufficient to catch all bad behavior that could expose the organization to risk</td>
<td>53.2%</td>
<td>24.8%</td>
<td>12.5%</td>
<td>9.5%</td>
</tr>
<tr>
<td>We have robust procedures in place that detect wrongdoing early enough to protect the organization from serious damage</td>
<td>24.8%</td>
<td>12.5%</td>
<td>9.5%</td>
<td>9.5%</td>
</tr>
<tr>
<td>We do not have specific procedures in place to manage conduct risk</td>
<td>12.5%</td>
<td>9.5%</td>
<td>9.5%</td>
<td>9.5%</td>
</tr>
<tr>
<td>I do not know whether we have specific procedures or not</td>
<td>9.5%</td>
<td>9.5%</td>
<td>9.5%</td>
<td>9.5%</td>
</tr>
</tbody>
</table>

3. Cloud risk and compliance

Many companies are considering moving, or have moved, business processes to the cloud, but managing cloud risks and compliance is not always a top priority during a transition. Challenges are often related to where exactly information is located, who has access to it and how it is protected. The potential repercussions of not managing end-to-end cloud risks include:

- Unintentional information disclosure
- Increased costs
- Regulatory penalties
- Inability to increase use of cloud solutions

In order to address cloud risk and compliance, management must start early with upfront development of a cloud solution with a compliance and risk mindset to decrease exposure and increase effectiveness. Furthermore, beginning with an established standard can help your organization better understand and mitigate cloud risks.
A cloud assessment from an experienced advisor can also evaluate your cloud governance program, identifying any potential weaknesses or gaps. Perhaps most importantly, involving all key stakeholders from the outset is a critical element to developing a compliant and secure cloud framework. Technology as a whole has become so pervasive and critical to all business functions, and therefore, each function should have a hand in identifying and managing risks.

### 4. Technology risk transformation

Many organizations are going through digital or finance transformation initiatives, implementing new technology systems and solutions. However, corporate board members and senior management are generally not satisfied with the level of information provided by technology functions within their organizations. Without full alignment of the risk management function reporting by the three lines of defense, senior management and the board cannot have a holistic perspective on risk. Common challenges include:

- Information that is either too granular or lacks prioritization
- Increased total cost of compliance
- Lack of confidence in management to effectively manage risk

To better manage these risks, management can leverage existing technology risk assessments or implement one to provide a comprehensive inventory of technology assets, as well as an opportunity to identify emerging risks and prioritize areas of focus. An established IT or information security framework can also ensure that technology investments and output are supporting organizational objectives and help develop a common control framework.

In addition, identifying key performance indicators (KPIs) and key risk indicators (KRIs) can provide additional insight into managing technology risks. Furthermore, developing consistent dashboards creates more visibility and reveals trending data, which can be communicated easily to boards and management. By identifying common controls within your technology environment and among the three lines of defense, your organization can take a “test once-use many” approach, which can minimize the total cost of compliance.

### 5. Rise of data privacy regulations

Data privacy is a critical concern for many middle market organizations, as new and planned legislation requires significant changes to how companies manage and store customer data. Companies are beginning to realize that privacy regulations such as the EU’s General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) will affect how they do business, but many may not understand that more laws are coming. This shift toward privacy can create several issues, including:

- Expensive fines if found in noncompliance
- Loss of market trust, customers and revenue
- Required transparency of privacy practices in all transactions
- New processes and procedures around data handling
Successfully responding to these challenges includes evaluating compliance with privacy laws for all geographies and retaining external counsel that specializes in data privacy laws. Current data should be inventoried and data handling and processing should be assessed, with processes updated as necessary to ensure compliance with all applicable regulations. Finally, review any data shared with third parties including business partners, advertisers and hosting providers, as you can face sanctions if they do not comply with privacy laws.

Not surprisingly, responses from our webcast attendees regarding data privacy preparedness were extremely varied. Many do not yet understand GDPR-style laws or believe new similar laws would be problematic. Conversely, many also think that new laws would either be manageable or have a negligible effect on current operations.

### What impact would new GDPR-style privacy laws in multiple U.S. states have on your business?

<table>
<thead>
<tr>
<th>Perception</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown. We do not understand the full privacy requirements and don’t know the impact.</td>
<td>25.9%</td>
</tr>
<tr>
<td>Manageable. We’ve planned for such laws and will be able to adjust quickly.</td>
<td>25.9%</td>
</tr>
<tr>
<td>Problematic. We are aware of changes we’d need to make and know that they would be difficult and expensive.</td>
<td>24.8%</td>
</tr>
<tr>
<td>Negligible. We have very little sensitive data, or have already become compliant with such privacy laws.</td>
<td>18.8%</td>
</tr>
<tr>
<td>Dreadful. We know full well the cost and business interruptions will be significant.</td>
<td>4.6%</td>
</tr>
</tbody>
</table>

**Conclusion**

In an increasingly volatile political and risk environment, preparation is key. Addressing these five emerging threats can help you fix vulnerabilities and improve decision-making, and ultimately develop a comprehensive and proactive risk strategy to be ready for what’s ahead.